Supplemento ordinario alla "Gazzetta Ufficiale,, n. 180 del 2 agosto 2008 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Sabato, 2 agosto 2008** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00186 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00198 ROMA - CENTRALINO 06 85081

N. 184

MINISTERO DELLA GIUSTIZIA

DECRETO 17 luglio 2008.

Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, in sostituzione del decreto del Ministro della giustizia 14 ottobre 2004, pubblicato nel supplemento ordinario n. 167 alla *Gazzetta Ufficiale* n. 272 del 19 novembre 2004.

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELLA GIUSTIZIA

DECRETO 17 luglio 2008.

Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, in sostituzione del decreto del Ministro della giustizia 14 ottobre 2004, pubblicato nel supplemento ordinario n. 167 alla *Gazzetta Ufficiale* n. 272 del 19 novembre 2004.

IL MINISTRO DELLA GIUSTIZIA

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante <<Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della Legge 23 ottobre 1992, n. 421>> e successive modificazioni;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n.445, recante << Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A) e successive modificazioni;

Visto il decreto ministeriale 27 marzo 2000, n. 264, recante <<Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari>>;

Visto il decreto del Presidente della Repubblica 13 febbraio 2001, n.123, recante <<Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti>> e successive modificazioni;

Visto il decreto ministeriale 24 maggio 2001;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante <<Codice in materia di protezione dei dati personali>> e successive modificazioni;

Visto il decreto del Ministro della Giustizia 14 ottobre 2004, recante <<Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile>> e, in particolare, l'articolo 61, secondo il quale << le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale>>.

Visto il decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale e successive modificazioni;

Rilevata la necessità di adeguare le regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, sostituendo il decreto del Ministro della Giustizia 14 ottobre 2004;

Sentito il Centro nazionale per l'informatica nella pubblica amministrazione;

Sentito il Garante per la protezione dei dati personali;

DECRETA

CAPO I
PRINCIPI GENERALI

Art. 1
(Ambito di applicazione)

1. Il presente decreto stabilisce le regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile di cui all'articolo 3, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001 n.123.

Art. 2
(Definizioni)

1. Ai fini del presente decreto si intendono per:
   a) SICI: sistema informatico civile come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n. 123;
   b) gestore centrale: struttura tecnico-organizzativa che, nell'ambito del dominio giustizia, come definito all'articolo 1, comma 1, lettera *e)* del D.P.R. 13 febbraio 2001, n. 123, fornisce i servizi di accesso al SICI ed i servizi di trasmissione telematica dei documenti informatici processuali fra il SICI ed i soggetti abilitati, secondo le norme riportate nel presente decreto;
   c) gestore locale: sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o all'ufficio notifiche esecuzioni e protesti (UNEP), ed i servizi di trasmissione telematica dei documenti informatici processuali fra il gestore centrale ed il singolo ufficio giudiziario o UNEP;
   d) certificazione del difensore: attestazione al difensore di iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati ovvero di possesso della qualifica che legittima l'esercizio della difesa e l' assenza di cause ostative allo svolgimento dell'attività difensiva;
   e) punto di accesso: struttura tecnico-organizzativa che fornisce ai soggetti abilitati, esterni al SICI, i servizi di connessione al gestore centrale e di trasmissione telematica dei documenti informatici relativi al processo, nonché la casella di posta elettronica certificata, secondo le regole tecnico-operative riportate nel presente decreto;
   f) autenticazione: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, contenente un certificato di autenticazione, secondo la previsione dell'art.62.
   g) firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 23 gennaio 2002, n.10.
   h) fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, ovvero le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo.
   i) soggetti abilitati: tutti i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:

1.1 soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice.

1.2 soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali.

1.3 soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici.

1.4 soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli UNEP

j) casella di posta elettronica certificata per il processo telematico (CPECPT): indirizzo elettronico, per il processo telematico, dei soggetti abilitati.

Art. 3

(Gestore centrale)

1. Il gestore centrale è il punto unico di interazione, a livello nazionale, tra il SICI ed i soggetti abilitati esterni.
2. Il gestore centrale è attivo presso il Ministero della giustizia.

Art. 4

(Gestore locale)

1. Il gestore locale è parte del sistema informativo dell'ufficio giudiziario e dell'UNEP, come definito nel decreto ministeriale del 24 maggio 2001, e rispetta i requisiti tecnici ed organizzativi definiti in tale ambito.
2. I gestori locali sono attivi presso le sale server dove sono gestiti i sistemi informativi degli uffici giudiziari e degli UNEP.

Art. 5

(Sistemi informatici di gestione della cancelleria e dell'UNEP)

1. Il sistema informativo di gestione delle cancellerie civili è costituito dall'infrastruttura hardware e software di gestione dei registri e dei fascicoli informatici.
2. Il sistema informativo di gestione degli UNEP è costituito dall'infrastruttura hardware e software per la gestione delle notifiche.

Art. 6

(Punto di accesso)

1. I soggetti abilitati esterni accedono al SICI tramite un punto di accesso, che può essere attivato esclusivamente dai soggetti pubblici di cui al comma 5 e dai soggetti privati di cui al comma 6. Ciascun soggetto può avvalersi di un solo punto di accesso.

2. I punti di accesso forniscono un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema e a non comprometterne i livelli di servizio, nel rispetto dei requisiti tecnici di cui all'articolo 30.
3. La violazione, da parte di un punto di accesso, dei livelli di sicurezza e di servizio, comporta la sospensione ad erogare i servizi fino al ripristino di tali livelli.
4. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.
5. I soggetti pubblici che possono attivare e gestire uno o più punti di accesso sono:
   a) I consigli dell'ordine degli avvocati, ciascuno limitatamente ai propri iscritti;
   b) Il Consiglio nazionale forense, limitatamente ai propri iscritti e agli iscritti dei consigli dell'ordine degli avvocati che glie ne fanno delega;
   c) Il Consiglio nazionale del notariato, limitatamente ai propri iscritti;
   d) L'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;
   e) Il Ministero della giustizia per i soggetti abilitati interni e, in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui ai punti a) e b);
   f) Il Ministero della giustizia, in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui al comma 6, al solo fine di garantire l'accesso agli esperti e ausiliari del giudice.
6. I soggetti privati che attivano e gestiscono un punto di accesso hanno i seguenti requisiti:
   a) forma di società per azioni;
   b) capitale sociale e requisiti di onorabilità di cui al decreto legislativo 1° settembre 1993, n. 385, articolo 25, comma 1.

Art. 7
(Certificazione dei difensori)

1. La certificazione del difensore è svolta dal punto di accesso, qualora questo sia gestito da un Consiglio dell'ordine degli avvocati o dal Consiglio nazionale forense, oppure dal gestore centrale sulla base di copia dell'albo fornita al Ministero della giustizia dai consigli dell'ordine degli avvocati e dal Consiglio nazionale forense.
2. L'aggiornamento della copia dell'albo avviene entro 72 ore dalla comunicazione, dei provvedimenti di pertinenza, all'interessato.
3. Il Consiglio nazionale forense compie il servizio di certificazione dei difensori per i propri iscritti o per gli iscritti dei consigli dell'ordine, su delega di questi ultimi.

Art. 8
(Accesso dei soggetti abilitati esterni privati)

1. Per il difensore delle parti è necessaria, ai fini dell'accesso al SICI, l'autenticazione presso il punto di accesso di cui al capo quarto e la certificazione di cui all'articolo 7.
2. Il SICI consente al difensore l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito e permette, negli altri casi, l'acquisizione delle sole informazioni necessarie per la costituzione in giudizio.
3. In caso di delega, rilasciata ai sensi dell'articolo 9 regio decreto legislativo 27 novembre 1933, n. 1578, il SICI consente all'avvocato delegato l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dall'avvocato delegante, previa comunicazione, a cura di parte, di copia della delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della revoca della delega.
4. La delega, sottoscritta con firma digitale, è rilasciata in conformità al modello previsto dall'articolo 56.
5. Gli esperti e gli ausiliari del giudice accedono al SICI nel limite dell'incarico ricevuto e della autorizzazione, concessa dal giudice, alla consultazione e alla copia degli atti.
6. A seguito dell'autenticazione, viene trasmesso al gestore centrale il codice fiscale del soggetto abilitato esterno privato.

Art. 9
(Accesso dei soggetti abilitati esterni pubblici)

1. Il punto di accesso autentica il soggetto abilitato esterno pubblico e trasmette il relativo codice fiscale al gestore centrale.
2. I dati, di cui al comma 1, sono utilizzati per individuare i privilegi di accesso alle informazioni contenute nel SICI.
3. Il SICI consente agli avvocati e procuratori dello Stato l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione.

Art. 10
(Accesso dei soggetti abilitati interni)

1. I soggetti abilitati interni accedono al SICI attraverso il Sistema Pubblico di Connettività (SPC) e attraverso il punto di accesso del Ministero della giustizia.

CAPO II
GESTIONE DELLA POSTA ELETTRONICA

Art. 11
(Casella di posta elettronica certificata del processo telematico)

1. I soggetti abilitati esterni, per utilizzare i servizi di trasmissione telematica dei documenti informatici, dispongono di un indirizzo elettronico e della relativa casella di posta elettronica certificata del processo telematico, CPECPT, forniti e gestiti dal punto di accesso, nel rispetto dei requisiti di cui all'articolo 12.
2. Ogni indirizzo elettronico, come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n.123, corrisponde ad una CPECPT.
3. Ad ogni soggetto che interagisce per via telematica con il SICI corrisponde un solo indirizzo elettronico.
4. Ogni CPECPT è abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale.

Art. 12
(Requisiti del servizio di gestione della CPECPT)

1. La CPECPT garantisce la ricezione dei messaggi e la loro disponibilità per trenta giorni, successivamente il messaggio è archiviato e sostituito da un avviso contenente i seguenti dati: identificativo univoco del messaggio, mittente, data, ora e minuti di arrivo.
2. L'avviso di cui al comma 1, contenente i riferimenti per il reperimento del messaggio, rimane disponibile per sei mesi.
3. Il servizio di posta elettronica certificata restituisce al mittente una ricevuta breve di avvenuta consegna per ogni documento informatico reso disponibile al destinatario, cui è associata l'attestazione temporale di cui all'articolo 45.
4. Salvo quanto previsto nel presente decreto, la posta certificata del processo telematico si conforma al D.P.R. 11 febbraio 2005 e alle relative regole tecniche.

Art. 13
(Registro generale degli indirizzi elettronici)

1. Il registro generale degli indirizzi elettronici, attivo presso il gestore centrale, contiene l'elenco di tutti gli indirizzi elettronici attivati dai punti di accesso.
2. Il registro generale degli indirizzi elettronici è accessibile ai soggetti abilitati esterni per il tramite dei punti di accesso e a tutti i soggetti abilitati interni, secondo le modalità previste dall'articolo 19.
3. All'indirizzo elettronico delle persone fisiche, sono associate le seguenti informazioni:

a) nome e cognome;
b) luogo e data di nascita;
c) codice fiscale
d) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
e) residenza;
f) domicilio;
g) stato dell'indirizzo: attivo, non attivo;
h) certificato digitale relativo alla chiave pubblica, da utilizzare per la cifratura;
i) consiglio dell'ordine o ente di appartenenza;
j) stato del difensore: attivo, non attivo.

4. All'indirizzo elettronico degli enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, sono associate le seguenti informazioni:
   a) denominazione sociale;
   b) codice fiscale;
   c) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
   d) sede legale;
   e) certificato digitale relativo alla chiave pubblica da utilizzare per la cifratura;
   f) stato dell'indirizzo: attivo, non attivo.

Art. 14

(Registrazione dei soggetti abilitati esterni al SICI)

1. L'accesso al SICI e la casella di posta elettronica si ottengono previa registrazione presso un punto di accesso.
2. La registrazione si ottiene con richiesta scritta, che il punto d'accesso conserva per almeno dieci anni.
3. Al momento della registrazione, il punto di accesso verifica l'identità del richiedente ed il relativo codice fiscale, e acquisisce i dati di cui all'articolo 13, commi 3 e 4.
4. I difensori delle parti presentano, all'atto della registrazione, un certificato, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine di appartenenza attesta l'iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati, oppure la qualifica che legittima all'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva.
5. Gli esperti e gli ausiliari del giudice presentano, all'atto della registrazione, il certificato della iscrizione all'albo dei consulenti tecnici o copia della nomina da parte del giudice dalla quale risulta che l'incarico non è esaurito.
6. Al momento della registrazione, i soggetti abilitati esterni comunicano al punto di accesso le seguenti informazioni:
   a) nome e cognome;
   b) luogo e data di nascita;
   c) codice fiscale
   d) residenza;
   e) domicilio;
   f) certificato digitale, relativo alla chiave pubblica, per la cifratura.
   g) consiglio dell'ordine di appartenenza.

I soggetti abilitati esterni comunicano al punto di accesso ogni variazione delle informazioni di cui alle lettere d), e), f) e g).

7. Le informazioni di cui al comma 6, unitamente alla qualità di difensore delle parti, di esperto o ausiliario del giudice, ed all'indirizzo elettronico assegnato e ad eventuali variazioni del suo stato, sono trasmesse dal punto di accesso al gestore centrale e, per i difensori delle parti, anche al consiglio dell'ordine di appartenenza.

Art. 15
(Obbligo di informazione)

1. I punti di accesso informano i titolari di indirizzi elettronici degli obblighi assunti in relazione al servizio offerto.

Art. 16
(Registro degli indirizzi elettronici del punto di accesso)

1. Il punto di accesso attiva un registro degli indirizzi elettronici che contiene l'elenco di tutti gli indirizzi elettronici emessi, revocati o sospesi dal punto di accesso.
2. Ad ogni indirizzo elettronico di persona fisica sono associate le informazioni di cui all'articolo 13, comma 3.
3. L'indirizzo elettronico di enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, associa le informazioni di cui all'articolo 13, comma 4.
4. Il difensore comunica al consiglio dell'ordine di appartenenza il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso, unitamente al proprio codice fiscale e ai dati identificativi del punto di accesso, ove tale comunicazione non sia stata fatta per suo nome e conto dal punto di accesso medesimo.
5. L'esperto o l'ausiliario del giudice comunica alla cancelleria competente il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso.
6. Il punto di accesso consente la consultazione del registro generale degli indirizzi elettronici di cui all'articolo 13 a tutti i soggetti abilitati ad accedere attraverso il punto di accesso stesso, nella propria area riservata, secondo le modalità previste dall'articolo 19.
7. Per i soggetti abilitati esterni pubblici, ciascun punto di accesso comunica al Ministero della giustizia, per via telematica, tutte le informazioni di cui all'articolo 13, commi 3 e 4, ed ogni loro variazione, al fine dell'inserimento nel registro generale degli indirizzi elettronici.

Art. 17
(Comunicazioni dei consigli dell'ordine degli avvocati e del Consiglio nazionale forense)

1. Al fine dell'inserimento nei registri degli indirizzi elettronici, i consigli dell'ordine degli avvocati e il Consiglio nazionale forense comunicano al Ministero della giustizia ed ai punti di accesso di riferimento, le seguenti informazioni e le loro variazioni, per via telematica, relative ai difensori:
   a) nome e cognome;
   b) luogo e data di nascita;
   c) codice fiscale;
   d) domicilio;
   e) indirizzo elettronico, dichiarato e fornito dal punto di accesso;
   f) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
   g) dati identificativi del punto di accesso che fornisce il servizio di posta elettronica;
   h) stato del difensore: attivo, sospeso, cancellato, radiato; con indicazione di inizio efficacia del provvedimento e di fine efficacia nell'ipotesi di provvedimento temporaneo.
2. La comunicazione di cui al comma 1 è sottoscritta, con firma digitale, dal presidente del consiglio dell'ordine ovvero del Consiglio nazionale forense, o da un loro delegato.
3. La comunicazione di cui al comma 1 è strutturata in linguaggio *XML*, secondo il formato definito nel decreto ministeriale di cui all'articolo 52.
4. La comunicazione fatta dal punto di accesso gestito dal Consiglio dell'ordine degli avvocati o dal Consiglio Nazionale Forense vale quale adempimento degli obblighi di cui al comma 1.
5. La comunicazione di cui al comma 1 è inviata da una casella di posta elettronica certificata, univoca per ciascun consiglio dell'ordine degli avvocati, aderente alle specifiche tecniche riportate nell'allegato A, indicata con atto sottoscritto dal Presidente del Consiglio dell'Ordine.

Art. 18
(Requisiti tecnici dei registri degli indirizzi elettronici)

1. Il gestore centrale e i punti di accesso rendono disponibile una copia operativa dei propri registri degli indirizzi elettronici e mantengono l'originale inaccessibile dall'esterno.
2. Il gestore centrale ed i punti di accesso garantiscono la conformità tra la copia operativa e l'originale dei propri registri e risolvono tempestivamente qualsiasi difformità, registrandola in un apposito giornale di controllo.
3. Le operazioni che modificano il contenuto dei registri sono consentite unicamente al personale espressamente autorizzato e sono registrate in un apposito giornale di controllo.
4. La data, l'ora e i minuti, iniziali e finali, di ogni intervallo di tempo nel quale i registri non risultano accessibili dall'esterno, oppure sono indisponibili in una loro funzionalità, sono registrate in un apposito giornale di controllo.

5. Almeno una copia dei registri è conservata in locali di sicurezza, ubicati in luoghi diversi da quelli ove sono custoditi gli originali.

Art. 19

(Modalità di accesso ai registri degli indirizzi elettronici)

1. L'accesso ai registri degli indirizzi elettronici avviene secondo una modalità compatibile con il protocollo *LDAP*, definito nella specifica pubblica *RFC 1777* e successive modificazioni.
2. Il gestore centrale dell'accesso e i punti di accesso possono fornire modalità di accesso al proprio registro aggiuntive rispetto a quella prevista dal comma 1.
3. La struttura *LDAP* è specificata nei decreti ministeriali di cui all'articolo 62, comma 2.

CAPO III

ATTIVITA' DEL SICI

Art. 20

(Funzionamento e gestione del SICI)

1. La direzione generale per i sistemi informativi automatizzati del Ministero della giustizia (DGSIA) cura il funzionamento e la gestione del gestore centrale.
2. Il coordinamento interdistrettuale dei sistemi informativi automatizzati (CISIA) cura, attraverso l'amministratore di sistema, il funzionamento del gestore locale degli uffici di competenza.
3. Il dirigente amministrativo dell'ufficio giudiziario e dell'UNEP curano e sono responsabili, per l'ufficio di propria competenza, della consistenza dei dati.

Art. 21

(Attività del gestore centrale)

1. Il gestore centrale fornisce il servizio di consultazione del SICI e il servizio di trasmissione telematica degli atti. I soggetti abilitati esterni accedono ai servizi del gestore centrale esclusivamente attraverso il proprio punto di accesso.
2. Il gestore centrale è connesso ai punti di accesso mediante canali sicuri.
3. Nelle comunicazioni o notificazioni al difensore, il gestore centrale controlla, mediante il registro generale degli indirizzi elettronici, la certificazione del difensore. In caso di esito negativo del controllo, il gestore centrale inoltra la comunicazione o notifica, e trasmette all'ufficio giudiziario o all'UNEP un messaggio contenente l'esito del controllo.
4. Il gestore centrale associa automaticamente, ad ogni documento informatico pervenuto da un punto di accesso, una attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti, che è inserita in un messaggio inviato all'indirizzo elettronico del mittente.

5. Il gestore centrale associa automaticamente, ad ogni ricevuta di avvenuta consegna breve pervenuta da un punto di accesso, una attestazione temporale, comprensiva di data, ora e minuti di ricezione del relativo documento informatico da parte del destinatario, e trasmette questi dati al gestore locale dell'ufficio giudiziario competente.
6. Il gestore centrale utilizza, per gli adempimenti di cui ai commi 4 e 5, un servizio di attestazione temporale basato, con una differenza non superiore ad un minuto primo, sulla scala di tempo *UTC (IEN)*, determinata ai sensi dell'articolo 3, comma 1, della legge 11 agosto 1991, n. 273.
7. Il gestore centrale verifica l'assenza di virus informatici per ogni messaggio, in arrivo e in partenza.
8. Il gestore centrale, se riceve un messaggio privo dei dati necessari all'instradamento verso l'ufficio giudiziario o l'UNEP, genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio e l'indicazione degli elementi mancanti.
9. Il gestore centrale inoltra automaticamente tutti i documenti informatici provenienti dall'esterno del SICI e diretti verso il gestore locale dell'ufficio giudiziario o dell'UNEP, ed associa la attestazione temporale.
10. Il gestore centrale fornisce un servizio di inoltro automatico di tutti i documenti informatici ricevuti dall'interno del SICI verso l'indirizzo elettronico di destinazione.
11. Il gestore centrale fornisce il servizio di conservazione di tutti i messaggi inviati e ricevuti, associati alle relative attestazioni temporali, con le modalità previste dalla delibera CNIPA del 19 febbraio 2004, n.11. I supporti sono inviati, con periodicità mensile, ad un apposito centro di conservazione presso il Centro di gestione centralizzata del Ministero della giustizia, che ne assicura la conservazione per un periodo di cinque anni.
12. Il gestore centrale esegue la certificazione del difensore, qualora non sia già stata compiuta dal punto d'accesso.
13. Il gestore centrale fornisce un servizio per verificare lo stato delle notifiche e delle relative ricevute brevi di avvenuta consegna.

Art. 22

(Attività del gestore locale)

1. Il gestore locale fornisce il servizio di consultazione del sistema informatico dell'ufficio giudiziario, per i soggetti abilitati collegati attraverso il gestore centrale.
2. Il gestore locale, mediante il sistema informatico di gestione della cancelleria, fornisce il servizio di consultazione nei limiti dei privilegi di accesso dell'utente.
3. Il gestore locale trasmette i documenti tra i sistemi informatici dell'ufficio giudiziario o dell'UNEP ed il gestore centrale.
4. Il gestore locale fornisce una verifica della ricezione di tutti i documenti informatici ricevuti dal gestore centrale e delle relative attestazioni temporali.
5. Il gestore locale decifra i messaggi crittografati ricevuti, secondo le regole previste all'articolo 42.

6. Il gestore locale cifra, con le modalità di cui all'articolo 43, i documenti in uscita, facenti parte del fascicolo informatico, quando sono destinati a soggetti abilitati esterni
7. Il gestore locale verifica automaticamente, con il controllo della firma digitale, l'autenticità e l'integrità di ogni documento informatico ricevuto.
8. Il gestore locale verifica il rispetto dei formati e l'assenza di virus.
9. Il gestore locale rende disponibile il documento ricevuto al sistema informatico di gestione delle cancellerie civili o dell'UNEP, associandovi le informazioni dell'attività di verifica di cui al comma 8, per valutarne la ricevibilità.
10. Il gestore locale mantiene traccia, nei log di sistema, delle operazioni di consultazione da parte degli utenti e di eventuali interventi modificativi di atti e documenti, in conformità a quanto previsto per il monitoraggio del sistema dal D.M. 24 maggio 2001 e successive modificazioni.

Art. 23

(Attività del sistema informatico di gestione della cancelleria)

1. Il sistema informatico di gestione delle cancellerie civili cura l'accettazione del documento ricevuto, aggiornando il relativo registro ed il fascicolo informatico.
2. Il sistema informatico di gestione delle cancellerie civili invia, tramite il gestore locale ed il gestore centrale, all'indirizzo elettronico del mittente, una comunicazione di accettazione del documento informatico da parte della cancelleria oppure i motivi della mancata accettazione. La comunicazione contiene, se possibile, il numero di iscrizione a ruolo.

Art. 24

(Attività del sistema informatico di gestione dell'UNEP)

1. Il sistema informatico di gestione degli UNEP acquisisce i documenti informatici da notificare, procede alla loro notifica e li restituisce con la relata di notifica.

Art. 25

(Orario di disponibilità dei servizi)

1. Il gestore centrale ed i gestori locali garantiscono la disponibilità del servizio nei giorni feriali dalle ore otto alle ore ventitrè, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 26
(Requisiti tecnici di sicurezza)

1. Al gestore centrale si applicano le regole di sicurezza stabilite per il SICI e per il Sistema Pubblico di Connettività.
2. Per il gestore locale e per il fascicolo informatico si applicano le norme sulla sicurezza previste dal decreto del Ministero della giustizia del 24 maggio 2001.

Art. 27
(Requisiti tecnici relativi all'infrastruttura di comunicazione)

1. Il gestore centrale ed i gestori locali comunicano, tra loro, esclusivamente mediante il Sistema Pubblico di Connettività.
2. Il gestore centrale utilizza l'infrastruttura tecnologica resa disponibile nell'ambito del Sistema Pubblico di Connettività per le comunicazioni con l'esterno del dominio giustizia.

CAPO IV
ACCESSO AL SICI

Art. 28
(Funzionamento e gestione del punto di accesso)

1. Il funzionamento e la gestione dei punti di accesso è a carico dei soggetti pubblici o privati, in possesso dei requisiti di cui all'articolo 6.

Art. 29
(Funzionalità del punto di accesso)

1. Il punto di accesso fornisce ai soggetti abilitati esterni i servizi di consultazione del SICI e di trasmissione telematica degli atti.
2. Il punto di accesso fornisce il servizio di autenticazione dei soggetti abilitati, per l'accesso al SICI. Il punto di accesso, gestito dal consiglio dell'ordine degli avvocati di appartenenza o dal Consiglio nazionale forense, con l'autenticazione del difensore, esegue la certificazione di cui all'articolo 7.
3. La comunicazione tra la postazione informatica del soggetto abilitato esterno e il punto di accesso avviene mediante canale sicuro.
4. Il punto di accesso mantiene in linea i documenti informatici inviati fino a quando non riceve un avviso di consegna dal gestore centrale o dal punto di accesso di destinazione.

5. Il punto di accesso fornisce il servizio di ricezione, inviando, in risposta ad ogni documento informatico ricevuto dal gestore centrale o da un altro punto di accesso, una ricevuta breve di avvenuta consegna.
6. Il punto di accesso verifica l'assenza di virus informatici per ogni messaggio in arrivo e in partenza.
7. Il punto di accesso garantisce, per un periodo di cinque anni, la conservazione di tutti i messaggi inviati e ricevuti.
8. il punto di accesso mette a disposizione dei propri iscritti e del Ministero della Giustizia le statistiche di utilizzo dei propri servizi.

Art. 30

(Requisiti tecnici del punto di accesso)

1. L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche previste dalla carta nazionale dei servizi.
2. I punti di accesso stabiliscono le connessioni con il gestore centrale mediante un collegamento sicuro con mutua autenticazione come specificato nell'allegato A
3. Ciascun punto di accesso stabilisce con il gestore centrale un canale sicuro di comunicazione, che consente la reciproca autenticazione e riservatezza.
4. Il punto di accesso garantisce un livello di disponibilità del servizio pari al 99,5 per cento, su base quadrimestrale, dalle ore otto alle ore ventidue, nei giorni feriali, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.
5. Le procedure per la fornitura dei servizi attuate dal punto di accesso sono dettagliatamente documentate sul manuale operativo, previsto dall'articolo 33.
6. Tutte le azioni e le procedure di sicurezza attivate dal punto di accesso sono dettagliatamente documentate nel piano per la sicurezza, previsto dall'articolo 34.
7. La frequenza di salvataggio dei dati è almeno giornaliera.
8. Gli eventi significativi nel funzionamento del punto di accesso, sono registrati sul giornale di controllo, di cui all'articolo 35.
9. I canali di autenticazione del presente regolamento sono in *SSL* versione 3, con chiave a 1024 bit.
10. Il Punto di accesso deve verificare, prima di consentire qualunque operazione, la presenza della smart card nel lettore collegato alla postazione dell'utente, qualora la smart card risulti non inserita la sessione deve essere terminata immediatamente. Il punto di accesso deve gestire correttamente la chiusura della sessione.
11. Il punto di accesso mette a disposizione dei suoi utenti i servizi di consultazione esposti dal gestore locale a beneficio dei soggetti abilitati esterni.

Art. 31
(Elenco pubblico dei punti di accesso)

1. L'elenco pubblico dei punti di accesso, attivo presso il Ministero della giustizia, comprende le seguenti informazioni:
   a) identificativo del punto di accesso;
   b) sede legale del soggetto titolare del punto di accesso;
   c) nome secondo lo standard *X.500*;
   d) indirizzo internet;
   e) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo elettronico, numero di telefono e di fax;
   f) elenco dei numeri telefonici di accesso;
   g) manuale operativo;
   h) data di cessazione dell'attività.

Art. 32
(Iscrizione nell'elenco pubblico dei punti di accesso)

1. Il soggetto che intende costituire un punto di accesso inoltra, alla DGSIA, domanda di iscrizione nell'elenco pubblico dei punti di accesso.
2. Alla domanda sono allegate le dichiarazioni di:
   a) possesso dei requisiti di cui all'articolo 6;
   b) attestazione di affidabilità organizzativa e tecnica necessaria per svolgere il servizio di punto di accesso;
   c) attestazione relativa all'impiego di personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti;
   d) obbligo di fornirsi di: manuale operativo, piano per la sicurezza e giornale di controllo, secondo quanto previsto dagli articoli 33, 34 e 35;
   e) obbligo di garantire la sicurezza e l'integrità del servizio e dei dati di propria competenza;
   f) obbligo di compiere il processo di autenticazione dei soggetti abilitati ad esso afferenti, su mandato del Ministero della giustizia, conformemente all'articolo 30, comma 1;
   g) obbligo di comunicare, al Ministero della giustizia, la data di cessazione del servizio, con preavviso di sei mesi;
   h) informazione dei dati di cui all'articolo 31.
3. Il Ministero della giustizia decide sulla domanda, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.
4. Con il provvedimento di cui al comma 3, il Ministero della giustizia delega la responsabilità del processo di autenticazione dei soggetti abilitati esterni al punto di accesso.

5. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso, di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'articolo 6, comma 3.

Art. 33
(Manuale operativo)

1. Il punto di accesso utilizza un manuale operativo in cui sono definite le procedure applicate per effetto del presente decreto.
2. Il manuale operativo è pubblicato a cura del punto di accesso, per la consultazione in via telematica.
3. Il manuale operativo contiene almeno le seguenti informazioni:
   a) dati identificativi del punto di accesso e del relativo gestore;
   b) dati identificativi della versione del manuale operativo;
   c) responsabile del manuale operativo;
   d) definizione degli obblighi del titolare del punto di accesso e di coloro che vi accedono per l'utilizzo dei servizi;
   e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
   f) tariffe;
   g) modalità di autenticazione, registrazione e gestione degli utenti;
   h) modalità di attivazione e gestione degli indirizzi elettronici;
   i) modalità di gestione del registro degli indirizzi elettronici;
   j) modalità di accesso al registro degli indirizzi elettronici;
   k) politiche e procedure di sicurezza;
   l) procedure di gestione delle anomalie relative ai flussi di interfaccia con il gestore centrale.

Art. 34
(Piano per la sicurezza)

1. Il punto di accesso individua ed iscrive, nel giornale di controllo, il responsabile per la sicurezza, individuato nel responsabile del trattamento dei dati, ove designato.
2. Il responsabile di cui al comma 1 definisce il piano per la sicurezza che contiene almeno i seguenti elementi:
   a) struttura generale, modalità operativa e struttura logistica dell'organizzazione;
   b) descrizione dell'infrastruttura di protezione per ciascun immobile rilevante ai fini della sicurezza;
   c) collocazione dei servizi e degli uffici negli immobili dell'organizzazione;
   d) elenco del personale e sua distribuzione negli uffici;
   e) ripartizione e definizione delle responsabilità;
   f) descrizione delle procedure utilizzate nell'attività di attivazione delle utenze e, limitatamente ai punti di accesso, di rilascio di indirizzi elettronici;
   g) descrizione dei dispositivi installati;

h) descrizione dei flussi di dati;
i) procedura di gestione delle copie di sicurezza dei dati;
j) procedura di gestione dei disastri;
k) analisi dei rischi;
l) descrizione delle contromisure;
m) specificazione dei controlli.

Art. 35
(Giornale di controllo)

1. Il punto di accesso attiva il giornale di controllo, contenente l'insieme delle registrazioni effettuate automaticamente allorché si verificano le condizioni previste dal presente decreto.
2. Le registrazioni possono essere effettuate in modo indipendente, anche su distinti supporti e di diverso tipo.
3. La registrazione associa la data, l'ora e i minuti in cui è effettuata.
4. Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e da consentire la ricostruzione accurata di tutti gli eventi rilevanti per la sicurezza.
5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo sono archiviate con le modalità previste dal presente decreto e conservate per un periodo di cinque anni.

Art. 36
(Postazioni di lavoro dei soggetti abilitati esterni)

1. La postazione di lavoro dei soggetti abilitati esterni è l'insieme delle risorse hardware, software e di rete da loro utilizzate direttamente per la formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del SICI.
2. La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario alla gestione della firma digitale su smartcard, e all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi.
3. La postazione di lavoro dei soggetti abilitati esterni è dotata di software idoneo a verificare l'assenza di virus informatici per ogni messaggio in arrivo e in partenza.

CAPO V
TRASMISSIONE DI DOCUMENTI INFORMATICI TRA IL SICI ED ENTITÀ ESTERNE

Art. 37
(Principi normativi)

1. Nella trasmissione di documenti informatici nell'ambito del processo civile, trovano applicazione tutte le prescrizioni contenute nel decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nel decreto legislativo 23 gennaio 2002 n.10 e successive modificazioni.
2. I documenti informatici prodotti nel processo civile sono sottoscritti con firma digitale, nei casi previsti dall'articolo 4, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123.

Art. 38
(Ricezione del documento informatico)

1. Il documento informatico inviato da un soggetto abilitato esterno è ricevuto dal SICI nel momento in cui il gestore centrale lo accetta e associa l'attestazione temporale di cui all'articolo 21, comma 4.
2. Il documento informatico inviato da un soggetto abilitato interno è ricevuto dal soggetto abilitato esterno nel momento in cui il gestore centrale riceve la ricevuta di avvenuta consegna breve relativa al documento e associa l'attestazione temporale di cui all'articolo 21, comma 5.

Art. 39
(Orario dei servizi telematici di cancelleria)

1. Il SICI fornisce i servizi telematici di cancelleria, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 40
(Iscrizione a ruolo generale)

1. Il sistema informatico dell'ufficio giudiziario invia al difensore, che iscrive la causa a ruolo per via telematica, una comunicazione, recante il numero di ruolo del procedimento assegnato dall'ufficio.

Art. 41
(Dimensione del messaggio)

1. La dimensione massima del messaggio è di 10 Mb.

Art. 42
(Crittografia del messaggio)

1. Al fine della riservatezza del documento da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia basato sulla chiave pubblica del gestore locale cui è destinato il messaggio.
2. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato A del presente decreto.
3. I certificati digitali relativi alle chiavi pubbliche dei gestori locali sono pubblicate in un registro del gestore centrale dell'accesso.
4. Il registro di cui al comma 3 è accessibile in modalità *LDAP*.

Art.43
(Trasmissione e consultazione dei fascicoli)

1. Nel caso di richiesta di trasmissione o di consultazione, totale o parziale, di un fascicolo, il gestore locale, per garantire la riservatezza della comunicazione, utilizza un meccanismo di crittografia basato sulla chiave pubblica di cifratura del soggetto abilitato esterno di destinazione.
2. Nel caso di richiesta di copia conforme del fascicolo, totale o parziale, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.
3. I certificati digitali relativi alle chiavi pubbliche dei soggetti abilitati esterni sono disponibili nel registro generale degli indirizzi di cui all'art.13.
4. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato A, del presente decreto.

Art. 44
(Trasmissione delle sentenze)

1. L'originale della sentenza, redatta in formato elettronico dal giudice estensore o, ai sensi dell'articolo 119 delle norme di attuazione del codice di procedura civile, dal cancelliere o dal dattilografo da questi incaricato, è sottoscritta con firma digitale dall'estensore, previa verifica della conformità dell'originale alla minuta.
2. In caso di giudice collegiale, l'originale della sentenza è sottoscritto con firma digitale anche dal presidente e, a tal fine, la sentenza gli è trasmessa, in formato elettronico, dal giudice estensore o dal cancelliere.
3. Il cancelliere attesta il deposito della sentenza apponendo la data e sottoscrivendo la sentenza con la propria firma digitale.

Art. 45
(Comunicazioni e notificazioni)

1. La comunicazione per via telematica di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno avviene mediante inoltro del documento dal gestore locale al gestore centrale, che lo invia alla CPECPT del destinatario.
2. La notificazione telematica di documenti informatici tra difensori avviene, ove sussistano i presupposti di cui alla legge 21 gennaio 1994, n. 53, mediante inoltro del documento dal punto di accesso del mittente alla CPECPT del destinatario. A tale scopo il punto di accesso trasmette il messaggio con il documento da notificare al gestore centrale che, a sua volta, inoltra il messaggio ricevuto al punto di accesso di destinazione.
3. Le richieste di un'attività di notifica telematica da parte di un ufficio giudiziario sono inoltrate, mediante SPC, al sistema informatico dell'UNEP. Le richieste dei difensori sono inoltrate all'UNEP per il tramite del punto di accesso del mittente e del gestore centrale, nel rispetto dei requisiti dei documenti informatici provenienti dall'esterno. La notificazione di documenti informatici da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da ufficio giudiziario verso soggetti abilitati esterni
4. Il sistema informatico dell'UNEP, eseguita la notifica, trasmette per via telematica, a chi ha richiesto il servizio, il documento informatico con la relata di notifica, costituita dalla ricevuta elettronica, sottoscritta dall'ufficiale giudiziario con firma digitale.
5. Nell'ipotesi di cui all'articolo 6, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001 n. 123, l'ufficiale giudiziario provvede a notificare il duplicato del documento informatico, su supporto ottico non riscrivibile.
6. La consegna del documento informatico alla CPECPT del soggetto abilitato esterno è assicurata dai punti di accesso mediante l'invio al mittente di una ricevuta di avvenuta consegna breve.
7. Il gestore centrale, nella trasmissione di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno, associa automaticamente ad ogni ricevuta breve di avvenuta consegna una attestazione temporale contenente data, ora e minuti della ricezione che inoltra al gestore locale per l'inserimento nel fascicolo informatico.
8. Nelle notifiche tra difensori, il gestore centrale, ricevuto dal mittente il messaggio da notificare, associa automaticamente ad esso una prima attestazione temporale, che viene spedita alla CPECPT del mittente e, unitamente al messaggio, alla CPECPT del destinatario. La CPECPT del destinatario, ricevuto il messaggio, invia al gestore centrale la ricevuta breve di avvenuta consegna; il gestore centrale associa a quest'ultima una seconda attestazione temporale, che viene spedita alla CPECPT del destinatario e, unitamente alla ricevuta di avvenuta consegna breve, alla CPECPT del mittente.

CAPO VI
PAGAMENTI

Art. 46
(Pagamenti)

1. I pagamenti per via telematica, relativi agli atti giudiziari, si effettuano mediante il modello definito dal Ministero dell'economia e delle finanze.
2. Il pagamento può anche avvenire nelle forme di cui all'articolo 1 del D.P.R. del 1 marzo 2001, n.126.
3. Gli estremi del pagamento sono allegati alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio giudiziario.
4. Se il pagamento è effettuato a norma del comma 2 e con sistemi non telematici, l'originale cartaceo dell'attestazione di pagamento deve, in ogni caso, essere presentato per la prima udienza.

Art. 47
(Diritto di copia)

1. Il difensore nella richiesta di copia può chiedere l'indicazione dell'importo del diritto corrispondente che gli è comunicato, senza ritardo, dall'ufficio giudiziario.
2. Alla richiesta di copia è associato un numero identificativo che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel fascicolo informatico per consentire il versamento secondo le modalità previste dal D.P.R. 1 marzo 2001 n. 126.

Art. 48
(Registrazione, trascrizione e voltura degli atti)

1. La registrazione, la trascrizione e la voltura degli atti avvengono, in via telematica, nelle forme previste dall'articolo 73 del decreto del Presidente della Repubblica 30 maggio 2002, n.115.

Art. 49
(Pagamento dei diritti di notifica)

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'articolo 46.
2. L'UNEP rende pubblici, attraverso il gestore locale dell'ufficio, gli importi dovuti a titolo di anticipazione. Eseguita la notifica, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previa definizione del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

CAPO VII
ARCHIVIAZIONE E CONSERVAZIONE DELLE INFORMAZIONI

Art. 50
(Gestione del fascicolo informatico)

1. Il sistema di gestione del fascicolo informatico è la parte del sistema dell'ufficio giudiziario dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno dell'ufficio giudiziario.
2. Il fascicolo informatico contiene i documenti informatici e le relative informazioni quali: allegati, ricevute brevi di avvenuta consegna e attestazioni temporali.

Art. 51
(Archiviazione e conservazione dei documenti informatici degli uffici giudiziari e degli UNEP)

1. I fascicoli informatici relativi ai procedimenti in corso sono archiviati, per tutta la durata del procedimento, nell'archivio in linea dell'ufficio giudiziario secondo le modalità previste dal decreto ministeriale del 24 maggio 2001.
2. I fascicoli informatici relativi ai procedimenti esauriti sono soggetti a conservazione, presso il competente ufficio giudiziario, secondo le modalità previste dalla deliberazione del CNIPA del 19 febbraio 2004, n.11, per il periodo previsto dall'art. 41 del decreto legislativo 22 gennaio 2004, n.42, fatte salve le operazioni di scarto ivi previste.
3. I documenti informatici degli UNEP sono soggetti a conservazione, presso il competente ufficio, secondo le modalità e termini di cui al comma 2.

CAPO VIII
STANDARD E MODELLI DI RIFERIMENTO

Art. 52
(Formato dei documenti informatici)

1. Gli atti del processo in forma di documenti informatici sono redatti in formato PDF e sono corredati di informazioni in formato *XML*, secondo le specifiche tecniche determinate a norma dell'articolo 62, comma 2.
2. L'atto del processo in formato PDF, di cui al comma precedente, deve essere ottenuto da una trasformazione di un documento testuale e non deve avere restrizioni per le operazioni di selezione e copia di parti (non è ammessa la scansione di immagini).

Art. 53

(Formato dei documenti informatici allegati)

1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, ed hanno i seguenti formati: *.pdf, .odf, .rtf, .txt, .jpg, .gif, .tiff, .xml.*
2. E' consentito l'utilizzo dei formati compressi *.zip, .rar. e .arj,* purché contenenti file i nei formati previsti dal comma precedente

Art. 54

(Documenti probatori e allegati non informatici)

1. I documenti probatori e gli allegati depositati in formato non elettronico, sono identificati e descritti in una apposita sezione del documento informatico, secondo le specifiche tecniche determinate a norma dell'articolo 62, comma 2, e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati: numero di ruolo della causa, progressivo dell'allegato e indicazione della prima udienza successiva al deposito.

Art. 55

(Servizio di posta elettronica)

1. Il servizio di posta elettronica utilizzato dal gestore centrale dell'accesso e dai punti di accesso è conforme agli standard dei sistemi di posta elettronica compatibili con il protocollo di trasporto *SMTP* ed il formato dei messaggi *S/MIME.*

Art. 56

(Modelli di documenti informatici prodotti dai difensori)

1. I modelli dei documenti informatici prodotti dai difensori, riportati nei decreti ministeriali di cui all'articolo 62, comma 2, sono relativi ai seguenti atti:

a. atto introduttivo (citazione, ricorso, ricorso cautelare, ricorso per decreto ingiuntivo);
b. nota di iscrizione a ruolo;
c. comparsa di costituzione e risposta con eventuale domanda riconvenzionale ed eventuale richiesta di rinvio della prima udienza per la chiamata in causa del terzo;
d. deduzioni istruttorie a norma dell'articolo 184 del codice di procedura civile;
e. note autorizzate *ex* articolo 183, comma 5, del codice di procedura civile;
f. memorie autorizzate;
g. chiamata in causa del terzo;

h. istanza;
i. reclamo;
j. atti conclusivi (comparsa conclusionale, memoria di replica);
k. atto di pignoramento;
l. atto di intervento nell'esecuzione;
m. osservazioni al progetto di distribuzione;
n. istanza di fallimento;
o. istanza di insinuazione al passivo;
p. ricorso per insinuazione tardiva;
q. ricorso per opposizione allo stato passivo;
r. istanza di ammissione alla procedura di amministrazione controllata;
s. istanza di ammissione alla procedura di concordato preventivo;
t. istanza di concordato fallimentare;
u. dichiarazione di voto nelle procedure di amministrazione controllata o di concordato;
v. delega rilasciata ai sensi dell'articolo 9 del R.D. legislativo 27 novembre 1933, n. 1578.

Art. 57

(Modelli di documenti informatici prodotti dalla cancelleria)

1. I modelli dei documenti informatici prodotti dalla cancelleria, riportati nei decreti ministeriali di cui all'articolo 62, comma 2, sono relativi ai seguenti atti:
a. verbale di udienza;
b. biglietto di cancelleria;
c. richiesta di notifica;
d. richiesta di informazione o ordine di esibizione.

Art. 58

(Modelli di documenti informatici prodotti dal giudice)

1. I modelli dei documenti informatici prodotti dal giudice, riportati nei decreti ministeriali di cui all'articolo 62, comma 2, sono relativi ai seguenti atti:
a. provvedimento (sentenza, ordinanza, decreto);
b. dispositivo sentenza;
c. verbale di conciliazione.

Art. 59

(Modelli di documenti informatici prodotti dal consulente tecnico di ufficio)

1. I modelli dei documenti informatici prodotti dal consulente tecnico di ufficio, riportati nei decreti ministeriali di cui all'articolo 62, comma 2, sono relativi ai seguenti atti:
a. modello generico di consulenza;
b. stima di beni mobili;
c. stima di beni immobili;
d. stima di azienda.

Art. 60

(Modelli di documenti informatici prodotti dall'UNEP)

1. Il modello dei documenti informatici prodotti dall'UNEP, riportati nei decreti ministeriali di cui all'articolo 62, comma 2, sono relativi al seguente atto: relata di notifica.

CAPO IX

DISPOSIZIONI FINALI E TRANSITORIE

Art.61

(Adeguamento delle regole tecnico-operative)

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 62

(Disposizioni transitorie)

1. L'attivazione del processo telematico è preceduta da un decreto dirigenziale, che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.
2. Le caratteristiche specifiche della strutturazione dei modelli informatici saranno pubblicate, con uno o più decreti ministeriali, entro 180 giorni dalla data di entrata in vigore del presente decreto.
3. L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche della Carta Nazionale dei Servizi; possono essere utilizzati i dispositivi crittografici non conformi alla Carta Nazionale dei Servizi, purché emessi entro il 31 dicembre 2008.
4. L'art.22, comma 6, e l'art.43, comma 1, hanno efficacia a decorrere dall'entrata in vigore del decreto dirigenziale, che accerta l'idoneità delle attrezzature informatiche preposte allo scopo.
5. Gli atti del processo che hanno forma di documento informatico possono essere depositati anche nel formato disciplinato dall'art. 52, comma 1, del decreto ministeriale 14 ottobre 2004, fino al 31/12/2008.

Art.63

(Efficacia)

1. Il presente decreto acquista efficacia il trentesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana e dalla stessa data sostituisce il decreto del Ministro della giustizia 14 ottobre 2004, pubblicato nella Gazzetta Ufficiale della Repubblica italiana del 19 novembre 2004, n. 272.

Roma, 17 luglio 2008

Il Ministro: ALFANO

REGOLE TECNICO-OPERATIVE

PER L'USO DI STRUMENTI INFORMATICI E TELEMATICI

NEL PROCESSO CIVILE

ALLEGATO *A*

DEFINIZIONI E ACRONIMI

Nel presente capitolo è riportata la descrizione dei termini, degli acronimi e delle abbreviazioni usate nel documento.

Acronimo	*Descrizione*
CA	Certification Authority
CdO	Consiglio dell'Ordine
CPECPT	Casella di Posta Elettronica Certificata Processo Telematico
DTD	Document Type Definition
GC	Gestore Centrale
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MIME	Multipurpose Internet Mail Extensions
PCT	Processo Civile Telematico
PdA	Punto di Accesso
PECPT	Posta Elettronica Certificata Processo Telematico
PIN	Personal Identification Number
RDPIC	Ricevuta di presa in carico
ReGIndE	Registro Generale degli Indirizzi Elettronici
RPC	Remote Procedure Call
RUG	Rete Unitaria della Giustizia
RUPA	Rete Unitaria della Pubblica Amministrazione
S/MIME	Secure Multipurpose Internet Mail Extensions
SICI	Sistema Informativo Civile
SICC	Sistema Informatico del Contenzioso Civile
SICID	Sistema Informativo Cognizione Ordinaria CIvile Distrettuale
SIL	Sistema Informativo del Lavoro
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPC	Servizio Pubblico di Connettività
SSLv3	Secure Sockets Layer version 3
UG	Ufficio Giudiziario
UNEP	Ufficio Notifiche e Protesti
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

1 DESCRIZIONE DELL'ARCHITETTURA DEL SISTEMA

1.1 SCENARIO COMPLESSIVO ED ATTORI COINVOLTI

Il Processo telematico prevede il seguente scenario operativo:
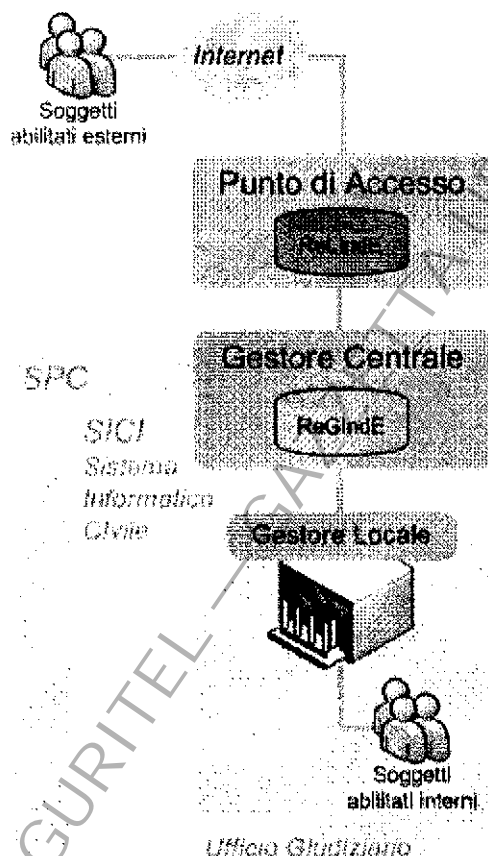
Figura 1 – Scenario operativo di riferimento

Il contesto applicativo prevede l'interazione tra i Soggetti Abilitati Esterni (avvocati e ausiliari del giudice) e i Sistemi di Gestione dei Registri (SGR) installati presso gli uffici giudiziari civili di primo e secondo grado.

Il soggetto abilitato esterno può:

- redigere e firmare l'atto di parte: a tal fine si avvale di uno o più strumenti per la redazione, la firma, la cifratura e l'imbustamento;
- depositare l'atto di parte, ricevendo in risposta la relativa attestazione temporale e successivamente le ricevute elettroniche di avvenuta presa in carico da parte dell'Ufficio Giudiziario e di inserimento nel fascicolo informatico;

- ricevere comunicazioni da parte dell'Ufficio Giudiziario nella propria "Casella di Posta Elettronica Certificata del Processo Telematico" (CPECPT);
- effettuare consultazioni dei fascicoli di propria pertinenza tramite i servizi di consultazione esposti dai Gestori Locali presso gli Uffici Giudiziari.

L'Avvocato interagisce con il SICI necessariamente per il tramite di un **Punto di Accesso Esterno** (PdA), presso cui è registrato come utente.

Il PdA è quindi l'unico fornitore dei servizi di interfacciamento del "dominio giustizia" per gli Avvocati, autorizzato ad operare su provvedimento dell'Amministrazione. Questo in quanto offre ai propri Utenti una schermatura dei protocolli e dei formati di interfaccia previsti dal PCT per il colloquio con gli Uffici Giudiziari (UG), salvaguardando i principi di sicurezza e di riservatezza (tramite **autenticazione forte**) alla base della specifica problematica applicativa.

Presso il PdA è attiva un'apposita anagrafica, che viene acceduta in fase di autenticazione, in fase di prelievo o consultazione dei messaggi provenienti dal SIC e in fase di deposito degli atti, per eseguire, se in possesso dell'albo elettronico del Consiglio dell'Ordine di appartenenza dell'Avvocato, la certificazione dello status del professionista.

Per quanto attiene alla ricezione di comunicazioni di cancelleria, il PdA fornirà all'avvocato una casella di posta elettronica certificata del Processo Telematico (CPECPT).

Il **Gestore Centrale** (GC) svolge servizi di cooperazione allo scambio di dati che, pur non entrando nel merito delle richieste ricevute, consentono di assicurare la correttezza della composizione delle buste prodotte e di tracciare tutti i flussi applicativi, verificando il completamento dei relativi cicli logici.

Provvede cioè ad indirizzare le richieste inoltrate dai PdA, e originate dagli Avvocati, verso gli UG destinatari e viceversa a smistare ai relativi PdA le risposte o le comunicazioni provenienti dagli UG, sopperendo, grazie ad una architettura logica e fisica particolarmente robusta, alla eventuale indisponibilità temporanea dei relativi sistemi di colloquio.

Il GC associa automaticamente, ad ogni documento informatico pervenuto da un punto di accesso, un'attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti. Questa è inserita in un messaggio inviato alla casella di posta elettronica di servizio del Punto di Accesso, che verifica la validità e provvede a renderla disponibile al mittente. Essendo una ricevuta a valore legale, il PdA informerà l'utente della ricezione anche in caso di anomalie formali del pacchetto.

Il GC esegue inoltre, in fase di deposito di un atto, la certificazione sostitutiva del difensore, nei casi in cui il PdA mittente non sia tenuto, o non sia stato delegato, alla gestione dell'albo dell'Ordine professionale di appartenenza dell'Avvocato mittente. A tal fine è previsto che ciascun Consiglio dell'Ordine inoltri al GC l'elenco aggiornato dei propri iscritti all'albo.

L'entità rappresentata come Ufficio Giudiziario coincide tecnicamente con il cosiddetto **Gestore Locale**, ossia l'insieme di tutti i servizi applicativi del Processo Telematico esposti sia verso il Gestore Centrale sia verso i soggetti abilitati ed i sistemi interni.

In particolare all'interno di questa componente vengono realizzati tutti i sottosistemi per:

- la gestione delle fasi di controllo e accettazione dell'atto di parte;
- l'invio di eventuali eccezioni al mittente;
- la gestione dei diritti di visibilità sui dati;
- l'invio dei biglietti di cancelleria.

Il Gestore Locale gestisce, infine, l'interfacciamento tra il *Repository* Documentale (la base dati documentale, contenente tra l'altro il fascicolo informatico) e i SGR per tutto ciò che concerne le operazioni a disposizione dei soggetti abilitati interni.

L'operatore di cancelleria e il Magistrato si interfacciano alle funzionalità del Processo Telematico rispettivamente attraverso i SGR e la "consolle del magistrato". Le evoluzioni dei SGR e la consolle del magistrato permettono infatti l'accesso al fascicolo informatico non più solo come storico degli eventi, ma anche nel merito del contenuto degli atti di parte.

Il Cancelliere in particolare, interviene attraverso componenti specifiche previste dal SGR interessato, per gestire le eventuali situazioni di eccezione che si possono verificare in fase di ricezione, controllo e accettazione degli atti di parte.

1.2 BREVI CENNI ARCHITETTURALI

I flussi del Processo Telematico possono essere classificati per tipologia in:

- invii di documenti e messaggi
- consultazioni.

Dal punto di vista applicativo, la loro principale differenza è legata all'utilizzo di un differente protocollo di trasporto nella tratta tra PdA e GC. In particolare, per gli invii di documenti e messaggi, è previsto l'utilizzo di un meccanismo asincrono, basato sul protocollo SMTP, mentre per le consultazioni, si prevede l'utilizzo di soli meccanismi sincroni, basati su HTTPS.
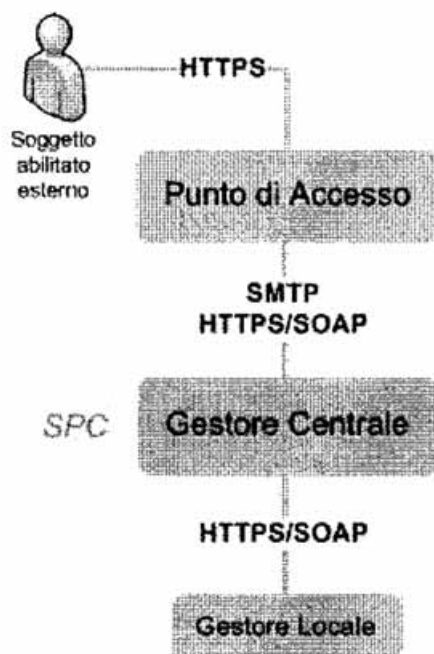
Figura 2 – Protocolli di trasporto

I soggetti abilitati esterni dovranno essere dotati di *token crittografici*[1] contenenti:

- il certificato per la firma elettronica, rilasciato da un certificatore accreditato, in modo da garantire che quelle determinate credenziali siano riferite ad una persona fisica la cui identità è garantita dall'insieme dei processi di identificazione attuati dal certificatore stesso;

[1] Tipicamente smart card

- il certificato di autenticazione, per la connessione al Punto di Accesso, rilasciato da una certification authority riconosciuta dal Punto di Accesso.

È pertanto possibile l'utilizzo di un solo token crittografico contenente entrambi i certificati oppure l'utilizzo di smart-card distinte. Sarà inoltre possibile dotarsi di più smart-card di autenticazione.

Il soggetto abilitato esterno deve essere dotato inoltre di un certificato di crittografia necessario per decifrare gli atti criptati; questo dovrà avere lunghezza di chiave di almeno 1024 bit e potrà coincidere con il certificato di autenticazione.

Dal punto di vista pratico, dunque, gli Avvocati opereranno su *client* dotati di dispositivo di lettura della *smart card* e, nel momento di connessione al PdA, per il deposito o la consultazione, inseriranno il proprio PIN e presenteranno le proprie credenziali con cui verranno autenticati dal servizio, creando così un canale sicuro basato su protocollo SSLv3.

Gli UG saranno inoltre dotati di chiave e certificati di cifratura[2] per consentire che gli atti depositati vengano cifrati sul *client* dell'avvocato, con il certificato pubblico dell'UG destinatario, e che solo quest'ultimo possa procedere a decifrare e leggere gli atti stessi.

I PdA e il GC sono attestati su internet e tra di loro sono instaurate connessioni sicure (SSLv3) in mutua autenticazione tra i server; pertanto l'interazione tra le due entità, tanto in caso di utilizzo del protocollo sincrono (per le consultazioni dei procedimenti giudiziari) che asincrono (per gli invii documentali), fruisce delle garanzie di sicurezza offerte da tale protocollo.

La tratta GC - UG avviene sempre in modalità sincrona (http/SOAP) utilizzando come canale di trasporto il Sistema Pubblico di Connettività (SPC); fruisce pertanto delle garanzie di sicurezza offerta da tale rete; nondimeno sono instaurate anche per questa tratta connessioni sicure (SSLv3) in mutua autenticazione tra i server.

[2] Si ipotizza che l'Amministrazione assuma in proprio la responsabilità della produzione e della distribuzione dei certificati server validi limitatamente alla operatività del Processo Telematico (in questo modo, ad esempio, potrebbero risultare più gestibili le problematiche di rinnovo dei certificati).

1.3 FLUSSI PRINCIPALI

Il presente paragrafo descrive i principali flussi del sistema.

1.3.1 Flusso di abilitazione e gestione utenze

La gestione delle utenze relative ai soggetti abilitati ad operare nel Processo Civile Telematico è regolamentata dagli articoli 14, 15 e 16.

Affinché il Gestore Centrale possa effettuare la certificazione dei difensori (come prevista dall'art. 7, comma 1), ed anche al fine del popolamento del Registro Generale degli Indirizzi Elettronici (ReGIndE), i Consigli degli Ordini degli Avvocati e il Consiglio Nazionale Forense debbono inviare al Gestore Centrale copia in formato elettronico dell'albo, sottoscritto con firma digitale (art. 17, commi 2 e 3).

Il Rappresentate dell'Ordine o un suo delegato (d'ora in avanti con il termine Rappresentante si intenderà colui che svolge le funzioni di Rappresentante del CdO per quanto attiene alla firma dell'albo elettronico) ha il compito di firmare digitalmente l'albo in formato elettronico ed inviarlo al GC tramite la casella di posta certificata del Processo Telematico (CPECPT) predisposta per questa funzione.

Il CdO è tenuto a comunicare al Ministero (DGSIA – Ufficio processo telematico) i dati di coloro che sono abilitati alla firma dell'albo, ovvero i dati del Rappresentante dell'ordine e di eventuali suoi delegati.

In particolare per ogni persona abilitata alla firma dell'albo elettronico dovranno essere comunicati:

- il codice fiscale
- il nominativo
- il certificato di firma digitale[3] del Rappresentante/delegato
- la tipologia di utente: ovvero se si tratta del *Rappresentante dell'Ordine* vero e proprio o di un suo *delegato.*

Non possono essere delegate a questa funzione persone afferenti alla struttura del gestore del PdA, sia esso pubblico o privato.

Per la funzionalità di invio dell'albo elettronico, ogni Consiglio dell'Ordine (CdO), nonché il Consiglio Nazionale Forense, debbono disporre di una casella di posta elettronica certificata del processo telematico (CPECPT) per scambiare messaggi con il GC.

L'accesso alla CPECPT è riservato al *Rappresentante del CdO* o ad un suo delegato, oppure ad un responsabile della struttura tecnica che gestisce il punto di accesso delegato dal CdO all'invio dell'albo.

[3] Il "Gestore Centrale" verifica che la comunicazione di variazione di *status* professionale degli Avvocati, non sia "semplicemente" firmata digitalmente, ma che lo sia esattamente col certificato digitale del Rappresentante/delegato del CdO di competenza

Tale casella di posta (CPECPT) non deve coincidere con quella eventualmente utilizzata dal Rappresentante in qualità di avvocato, ma deve essere una casella appositamente creata per svolgere le mansioni afferenti al Rappresentante stesso.

Si configurano quindi tre a casi, a seconda che il CdO sia titolare o meno di un PdA:

a) Se il CdO possiede un proprio Punto di Accesso, la CPECPT è creata sul proprio PdA; in questo caso l'indirizzo della CPECPT va comunicato alla DGSIA (Ufficio processo telematico) a cura del CdO. Il CdO può delegare, per l'operazione di invio albo, un responsabile della struttura tecnica che gestisce il proprio punto di accesso.

b) Qualora il CdO non possegga un proprio Punto di Accesso, il CdO può richiedere che la CPECPT sia creata sul punto di accesso del Ministero della Giustizia (PdA-MG); in questo caso il CdO invia una richiesta alla DGSIA (Ufficio processo telematico), che dovrà riportare il codice fiscale, il nominativo, il certificato di firma digitale del rappresentante. La DGSIA provvederà a creare l'account sul PdA-MG e a comunicarlo al CdO richiedente.

c) Qualora il CdO non possegga un proprio Punto di Accesso, può delegare un altro PdA all'invio dell'albo. La delega è comunque relativa al solo invio dell'albo, che dovrà in ogni caso essere firmato dal Rappresentate del CdO (o suo delegato). Il PdA delegato all'invio dell'albo provvederà a creare la CPECPT e a darne comunicazione al CdO.

In caso di delega all'invio ad un PdA (punto c) o ad un responsabile della struttura che gestisce il PdA pubblico (punto a), il CdO dovrà preventivamente comunicare al Ministero della Giustizia:

- tutte le indicazioni relative alla delega formale e specifica fornita;
- l'indirizzo della CPECPT utilizzata per l'invio dell'albo.

L'albo firmato dal Rappresentante del CdO (o un suo delegato) sarà quindi trasmesso al GC tramite la CPECPT predisposta a tale funzione.

Nel seguito vengono descritti i flussi abilitativi di Avvocati e CTU, i flussi di variazione dei dati e di cancellazione della registrazione invocati dagli utenti stessi. Vengono inoltre descritti i flussi di invio albo da parte dei CdO e CNF e invio di richieste di variazione status professionale.

Lo scambio di messaggi tra PdA, GC e CdO dei flussi descritti avviene per via telematica, tramite PECPT, e le comunicazioni sono strutturate in linguaggio XML, secondo il formato definito nel decreto di cui all'art. 62, comma 2.

Tutte le modifiche dei dati nei Registri degli Indirizzi sono visibili agli utenti a partire dal giorno lavorativo successivo a quello in cui vengono effettuate.

Registrazione e certificazione del soggetto abilitato esterno

Il diagramma di sequenza è riportato nella seguente figura:
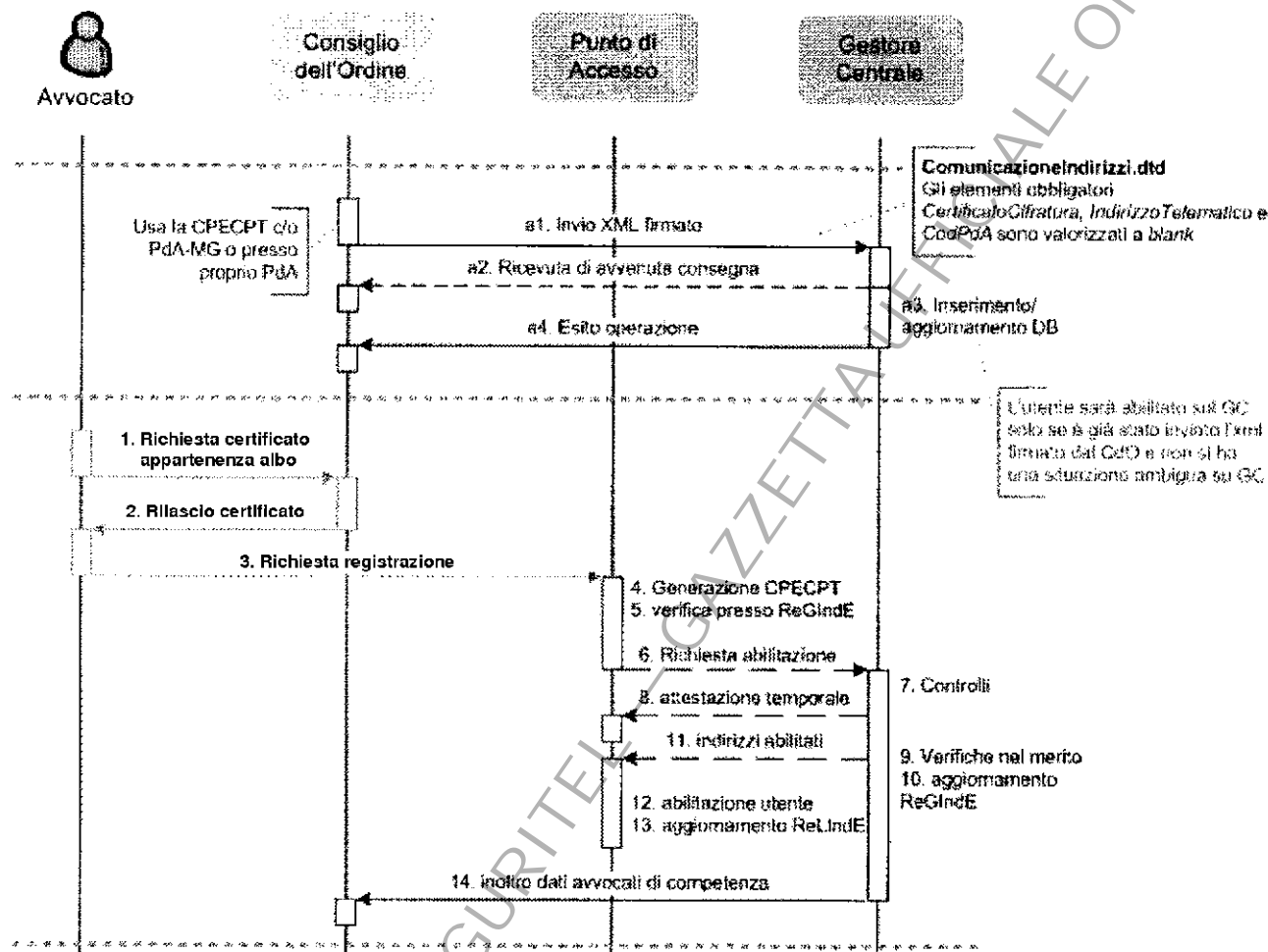
Figura 3 – Diagramma di sequenza relativo ai flussi di invio albo e gestione iscrizioni

Di seguito la descrizione del flusso riportato:

a1. il Consiglio dell'Ordine degli avvocati (o il Consiglio Nazionale Forense) invia alla casella di posta certificata del Gestore Centrale copia dell'albo, in formato elettronico, sottoscritta con firma digitale;

a2. il GC, alla ricezione della copia dell'albo, invia al CdO la Ricevuta di avvenuta consegna.

a3. Il Gestore Centrale quindi aggiorna il database di gestione dell'albo ed eventualmente aggiorna il ReGIndE nel caso l'avvocato sia già registrato;

a4. invia quindi l'esito dell'operazione al CdO.

Di seguito la descrizione del flusso relativo alla creazione di un'utenza, nel caso particolare di un avvocato:

1. L'avvocato si reca presso il proprio Consiglio dell'Ordine e richiede il certificato di appartenenza all'albo.
2. Ricevuto il certificato da parte del CdO,
3. l'avvocato consegna al Punto di Accesso prescelto una richiesta scritta di registrazione, accompagnata dal certificato di appartenenza all'albo e dalla chiave pubblica del proprio certificato di cifratura.
4. Il Punto di Accesso genera l'indirizzo elettronico dell'avvocato
5. e verifica che l'avvocato non abbia già un indirizzo elettronico nel Registro Generale degli Indirizzi.
6. Il Punto di Accesso invia quindi al Gestore Centrale una richiesta di abilitazione dell'avvocato, in un formato XML che comprende codice fiscale, indirizzo elettronico, consiglio dell'ordine, codice del PdA, chiave pubblica del certificato di cifratura e dati anagrafici dell'avvocato.
7. Il Gestore Centrale effettua i controlli formali sul messaggio:
8. in caso di errore nel formato del messaggio viene inviata una notifica di eccezione al PdA mittente ed il flusso viene interrotto; in caso di esito positivo invia un'attestazione temporale.
9. Il Gestore Centrale verifica il merito della richiesta. Se non è già presente nel ReGIndE verifica la presenza dell'utente nel database dell'albo per procedere alla registrazione e abilitazione dell' LDAP.
10. nel caso invece non sia presente, l'utente viene registrato nel ReGIndE, ma la registrazione non verrà attivata fino all'invio dei dati da parte del relativo CdO;
11. in caso di esito negativo dei controlli (ad esempio se l'avvocato è già presente nel ReGIndE) invia al Punto di Accesso un messaggio contenente l'anomalia; in caso di esito positivo invia al Punto di Accesso un file XML contenente gli indirizzi registrati.
12. Il Punto di Accesso riceve il file XML e a sua volta aggiorna il Registro Locale degli Indirizzi per quanto riguarda i dati di competenza del CdO (stato difensore). Si fa notare che l'inoltro del file XML da parte del GC al PdA avviene solamente nel caso in cui l'iscrizione dell'avvocato sia stata precedente all'invio dell'albo da parte del CdO.
13. e abilita l'avvocato (sempre dal giorno successivo, al pari del GC).
14. Il Gestore Centrale inoltra i dati degli avvocati di competenza di ciascun Consiglio dell'Ordine alle relative caselle di posta certificata.

Il flusso di creazione di un'utenza comporta variazioni sul Registro degli Indirizzi, e tratta esclusivamente invio di dati "anagrafici", non informazioni relative allo status del difensore.

Possono essere trattati sia "Avvocati" sia "CTU" (per quest'ultima tipologia di utenza non è prevista la fase di certificazione).

Variazione o cancellazione generata dall'utente (avvocato)

Di seguito il flusso previsto per la variazione dei dati anagrafici (modifica dei dati elencati all'art. 14, comma 6) generata da parte dell'utente stesso (nel caso di corretto invio dei messaggi)..

La cancellazione di un utente viene gestita come un caso particolare di variazione; anche in questo caso la richiesta può essere generata dall'utente stesso.
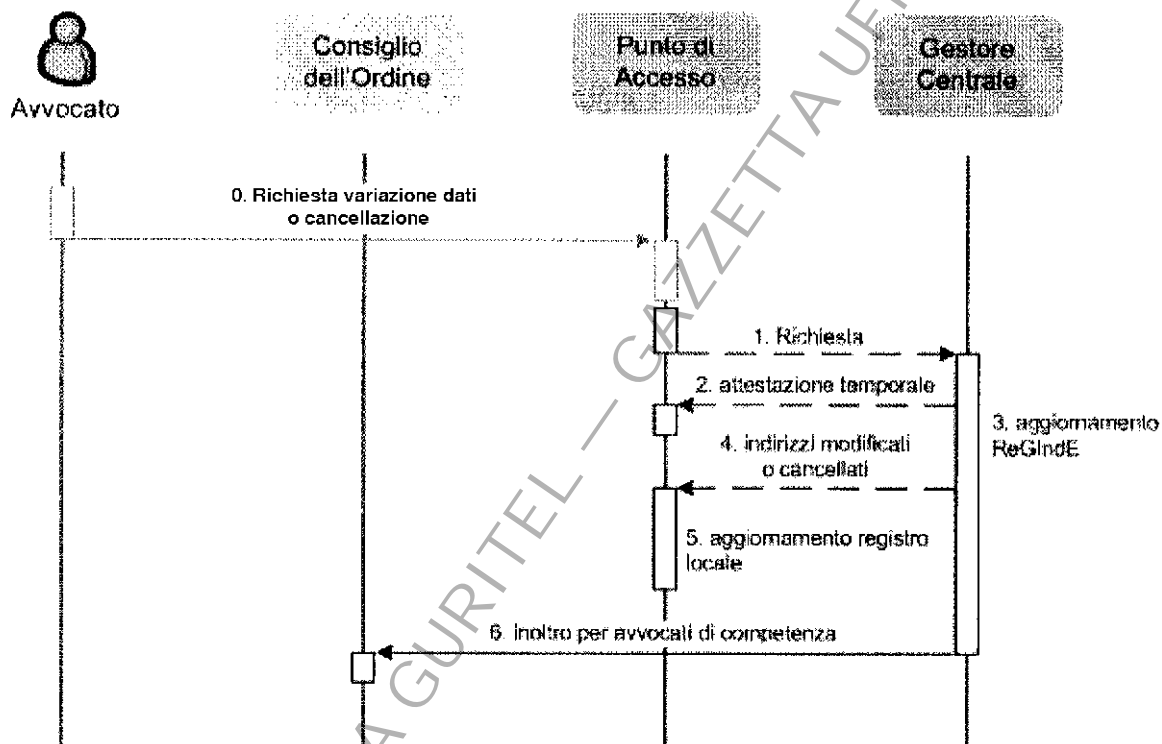
Figura 4 - Flusso di variazione utenza o cancellazione - generata dall'utente Avvocato

Di seguito una descrizione del flusso:

0. L'avvocato effettua la richiesta di variazione o di cancellazione presso il proprio Punto di Accesso;
1. Il Punto di Accesso invia al Gestore Centrale la richiesta, in un formato XML che comprende codice fiscale, indirizzo elettronico, consiglio dell'ordine, codice del PdA, chiave pubblica del certificato di cifratura e dati anagrafici dell'avvocato;
2. Il Gestore Centrale, dopo avere effettuato i controlli formali invia al Punto di Accesso un'attestazione temporale in caso di esito positivo, una notifica di eccezione altrimenti.

3. Quindi controlla il merito della richiesta ed in caso positivo si predispone all'aggiornamento del ReGIndE (che sarà operativo il giorno lavorativo seguente) con i dati dell'avvocato o la cancellazione (effettuata non fisicamente)
4. invia un file XML con i dati modificati o la conferma di cancellazione. In caso di esito negativo dei controlli il GC invia un messaggio contenente l'anomalia alla CPECPT del Punto di Accesso;
5. il Punto di Accesso riceve il file XML e a sua volta aggiorna la propria anagrafica;
6. il Gestore Centrale inoltra i dati degli avvocati di competenza di ciascun Consiglio dell'Ordine alle relative caselle di posta certificata.

Il caso previsto alla lettera g) dell'art. 14 comma 6 (modifica del Consiglio dell'Ordine) viene trattato come una richiesta di cancellazione, che deve essere seguita da una nuova richiesta di registrazione.

Allo stesso modo viene gestito anche il cambio di Punto di Accesso.

Variazione generata dal Consiglio dell'Ordine (solo per avvocati)

Per quanto riguarda gli avvocati, è prevista la variazione dello stato dell'avvocato, comunicata dal Consiglio dell'Ordine (ad esempio per una sospensione o per la radiazione) con l'invio di un file XML di variazione dati dell'Albo firmato digitalmente.

Il flusso previsto (nel caso di corretto invio dei messaggi) è il seguente:
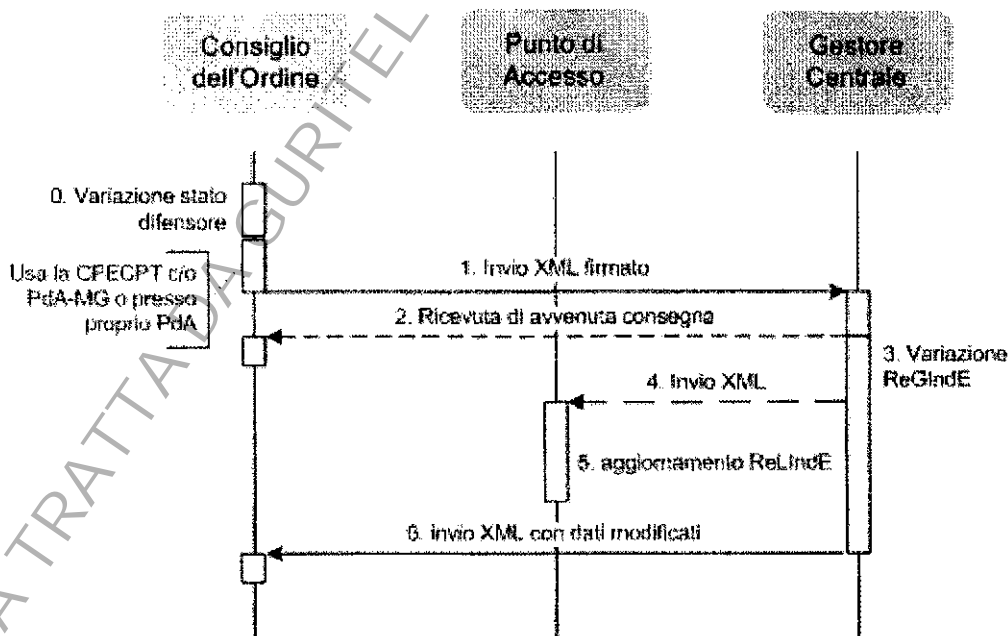
Figura 5 - Flusso di variazione utenza - generata dal CdO

Di seguito una descrizione del flusso:

0. Il Consiglio dell'Ordine varia lo stato del difensore e crea il file XML contenente i dati dell'avvocato e il nuovo stato ("attivo", "sospeso", "radiato");
1. il file XML viene firmato dal Presidente del CdO (o da un suo delegato) ed inviato alla casella di posta certificata del Gestore Centrale;
2. Il Gestore Centrale, dopo avere effettuato i controlli formali invia alla CPECPT del Consiglio dell'Ordine un'attestazione temporale in caso di esito positivo, una notifica di eccezione altrimenti.
3. Quindi controlla il merito della richiesta e in caso positivo aggiorna il ReGIndE (che sarà operativo il giorno lavorativo seguente) con i dati dell'avvocato.
4. Il Gestore Centrale inoltra al Punto di Accesso il file XML ricevuto dal Consiglio dell'Ordine.
5. Il Punto di Accesso aggiorna la propria anagrafica.
6. Il Gestore Centrale invia all'Ordine un file XML con i dati modificati. In caso di esito negativo dei controlli il GC invia un messaggio contenente l'anomalia alla CPECPT dell'Ordine.

Cancellazione generata dal Consiglio dell'Ordine (solo per avvocati)

Per quanto riguarda gli avvocati, è prevista la cancellazione di un avvocato dall'albo nei casi in cui l'avvocato cambi albo o cessi la propria attività. La cancellazione viene comunicata dal Consiglio dell'Ordine con l'invio di un file XML di cancellazione dati dell'Albo firmato digitalmente.

Per la descrizione del flusso si può far riferimento a Figura 5 tenendo presente che si tratta però di un'operazione di cancellazione :

0. Il Consiglio dell'Ordine crea il file XML di cancellazione contenente i dati dell'avvocato
1. il file XML viene firmato dal Presidente del CdO (o da un suo delegato) ed inviato alla casella di posta certificata del Gestore Centrale;
2. Il Gestore Centrale, dopo avere effettuato i controlli formali invia alla CPECPT del Consiglio dell'Ordine un'attestazione temporale in caso di esito positivo, una notifica di eccezione altrimenti.
3. Quindi controlla il merito della richiesta ed in caso positivo si predispone all'aggiornamento del ReGIndE (che sarà operativo il giorno lavorativo seguente) con i dati dell'avvocato o la cancellazione (effettuata non fisicamente)
4. Il Gestore Centrale inoltra al Punto di Accesso il file XML ricevuto dal Consiglio dell'Ordine
5. Il Punto di Accesso aggiorna la propria anagrafica.
6. Il Gestore Centrale invia all'Ordine un file XML con la conferma di cancellazione. In caso di esito negativo dei controlli il GC invia un messaggio contenente l'anomalia alla CPECPT del Punto di Accesso;

1.3.2 Redazione e deposito dell'atto di parte o dell'ausiliario del giudice

L'atto è un documento elettronico in formato PDF (redatto attraverso un qualsiasi word processor e convertito in PDF successivamente), mentre le informazioni di profilo necessarie alla cancelleria per definire il contesto nel quale collocare l'atto piuttosto che gli eventi di cancelleria ad esso associati sono contenute in un file XML a corredo denominato *DatiAtto.xml* la cui struttura è definita da appositi XSD (XML Schema Definition), che vengono pubblicati nel decreto previsto all'art. 62, comma 2.

L'atto (file PDF e *DatiAtto.xml*) ed i suoi allegati in formato elettronico, secondo i formati consentiti, debbono essere assemblati in una "busta" in formato MIME contenente:

1. le informazioni relative al depositante e le informazioni di instradamento del deposito nel contesto della porzione MIME denominata *InfoInoltro.xml*;
2. l'atto e i suoi allegati, cifrati per l'Ufficio Giudiziario di destinazione e quindi solo da questo visualizzabili (*Atto.enc*); il contenuto di *Atto.enc* è a sua volta un oggetto MIME nel contesto del quale sono contenuti, oltre alle informazioni di natura tecnica necessarie alla decifratura (chiave di sessione, riferimento al certificato):
   a. il file strutturato denominato *IndiceBusta.xml* contenente l'elenco dei contenuti da depositare e la loro tipologia (atto principale o allegato);
   b. il file *DatiAtto.xml* che descrive il profilo del documento da depositare;
   c. l'atto vero e proprio firmato digitalmente, indicato con il nome *CorpoAtto.pdf.p7m*;
   d. gli eventuali allegati all'atto depositato.

In figura è illustrato quanto sopra:
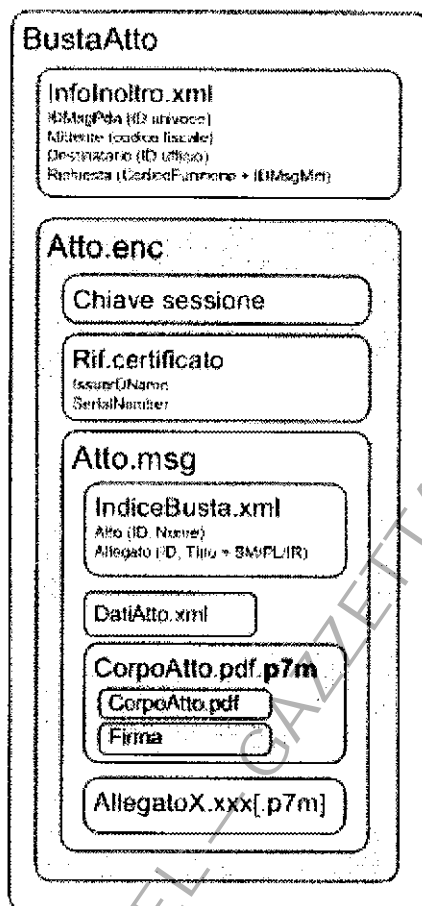
Figura 6 – Schema della struttura della Busta

I dettagli sulla firma e cifratura sono trattati al paragrafo 2.2.

Il file PDF contenente l'atto da depositare ed il relativo *DatiAtto.xml* devono essere firmati utilizzando un certificato digitale rilasciato da una *Certification Authority* (CA) accreditata dal CNIPA mentre sugli allegati la firma digitale è opzionale.

È compito del software utilizzato dall'utente esterno controllare che il codice fiscale presente nel certificato di firma associato all'atto principale sia il medesimo di quello inserito in DatiAtto.xml.

Il formato degli atti e della busta di deposito sopra descritto è valido per tutte le tipologie di deposito che possono essere effettuate ovvero per atti degli avvocati e degli ausiliari del giudice.

Una volta che la busta è pronta, questa può essere trasmessa attraverso la funzione di "deposito atto" messa a disposizione dal PdA, secondo le modalità che questo ha sviluppato per i propri utenti.

Nella figura che segue è riportato il diagramma di sequenza che illustra il flusso di deposito e di ricezione dei relativi esiti:
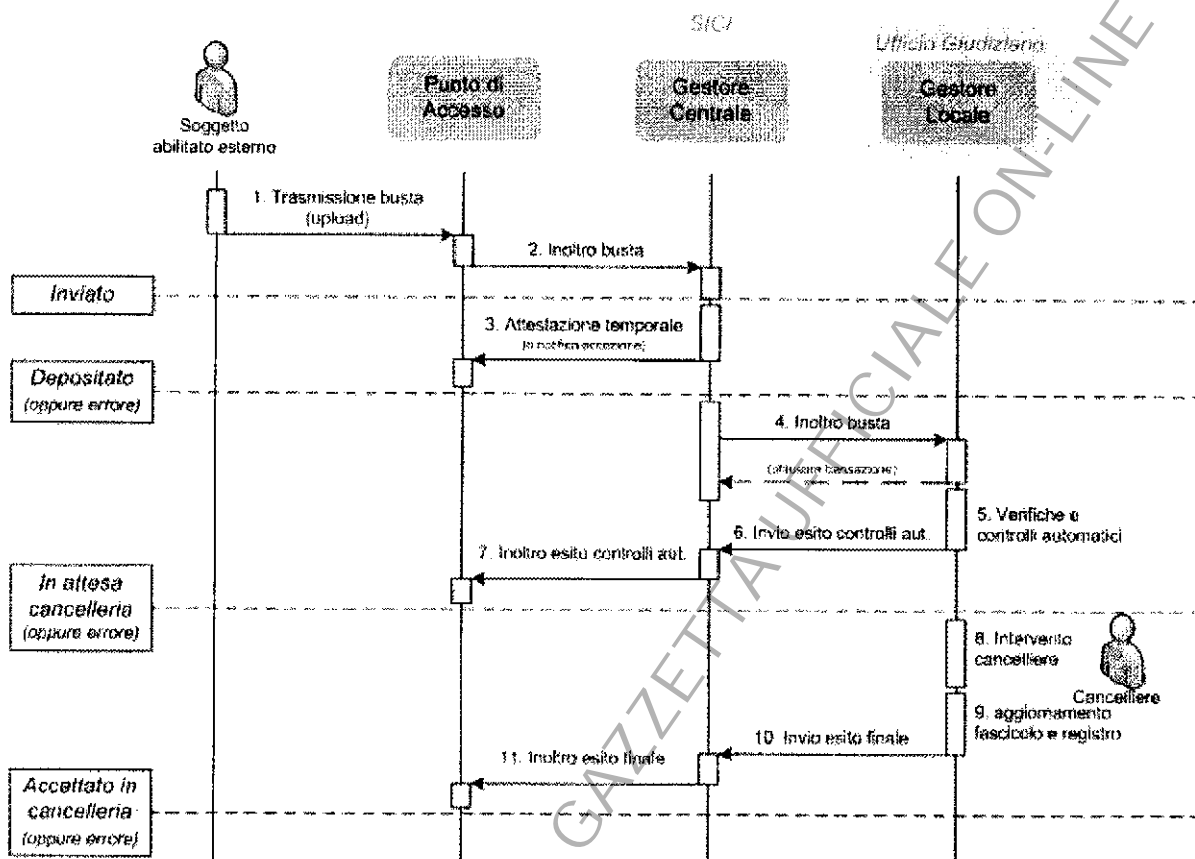
Figura 7 – Diagramma di sequenza del flusso di deposito

Questa la spiegazione del diagramma sopra riportato.

1. il soggetto abilitato esterno si connette via internet con il proprio PdA, si autentica e attiva la funzionalità di trasmissione della busta criptata, tipicamente realizzata tramite upload;
2. il PdA effettua il controllo antivirus e inoltra la busta al GC,
3. il quale risponde, se il messaggio è corretto, con l'attestazione temporale, che ha valore legale per la verifica dei termini di scadenza per la presentazione dell'atto, salvo verifica di buon fine dell'atto medesimo presso l'UG (verifica delle condizioni minime di accettabilità dell'atto).

I flussi 2 e 3 avvengono utilizzando il protocollo SMTP.

4. il GC inoltra la busta al GL, utilizzando un canale sincrono (HTTP/SOAP);
5. il GL effettua i controlli automatici previsti
6. ed invia immediatamente al GC l'esito di tali controlli (si veda paragrafo 2.4);
7. il GC inoltra tale esito al PdA;
8. a seguito dell'intervento del cancelliere,
9. il sistema aggiorna il registro di cancelleria e il fascicolo informatico, inserendovi l'atto in formato elettronico, che da questo momento è consultabile on-line;

10. il sistema invia in automatico l'esito finale dell'operazione al GC,
11. il GC inoltra tale esito al PdA.

È compito del PdA presentare al soggetto abilitato i messaggi di risposta ricevuti.

Il Ministero della Giustizia, nell'ambito delle regole tecnico-operative, fornisce le necessarie specifiche (WSDL, DTD, XSD e quant'altro) per consentire a tutti i fornitori di software di realizzare gli strumenti necessari per predisporre l'atto informatico e la relativa busta, nonché per integrare le relative funzioni nei software di gestione degli studi professionali, secondo la logica "application-to-application".

Tutti i software realizzati dal Ministero, e scaricabili dal sito www.processotelematico.giustizia.it, sono disponibili a soli fini dimostrativi e prototipali, in particolare al fine di agevolare lo sviluppo dei software esterni che interagiscono con il Processo Telematico.

1.3.3 Comunicazioni di cancelleria

La funzione di invio di un biglietto di cancelleria prevede un flusso di trasmissione di una comunicazione, prodotta dal Cancelliere, alle CPECPT di uno o più soggetti abilitati esterni[4], e di un flusso di risposta, di direzione opposta, innescato dalla emissione delle singole ricevute di presa in carico delle comunicazioni da parte dei PdA gestori delle CPECPT interessate.

Il diagramma di sequenza è riportato nella seguente figura.

[4] In caso di invio a più soggetti, gli invii sono comunque separati.
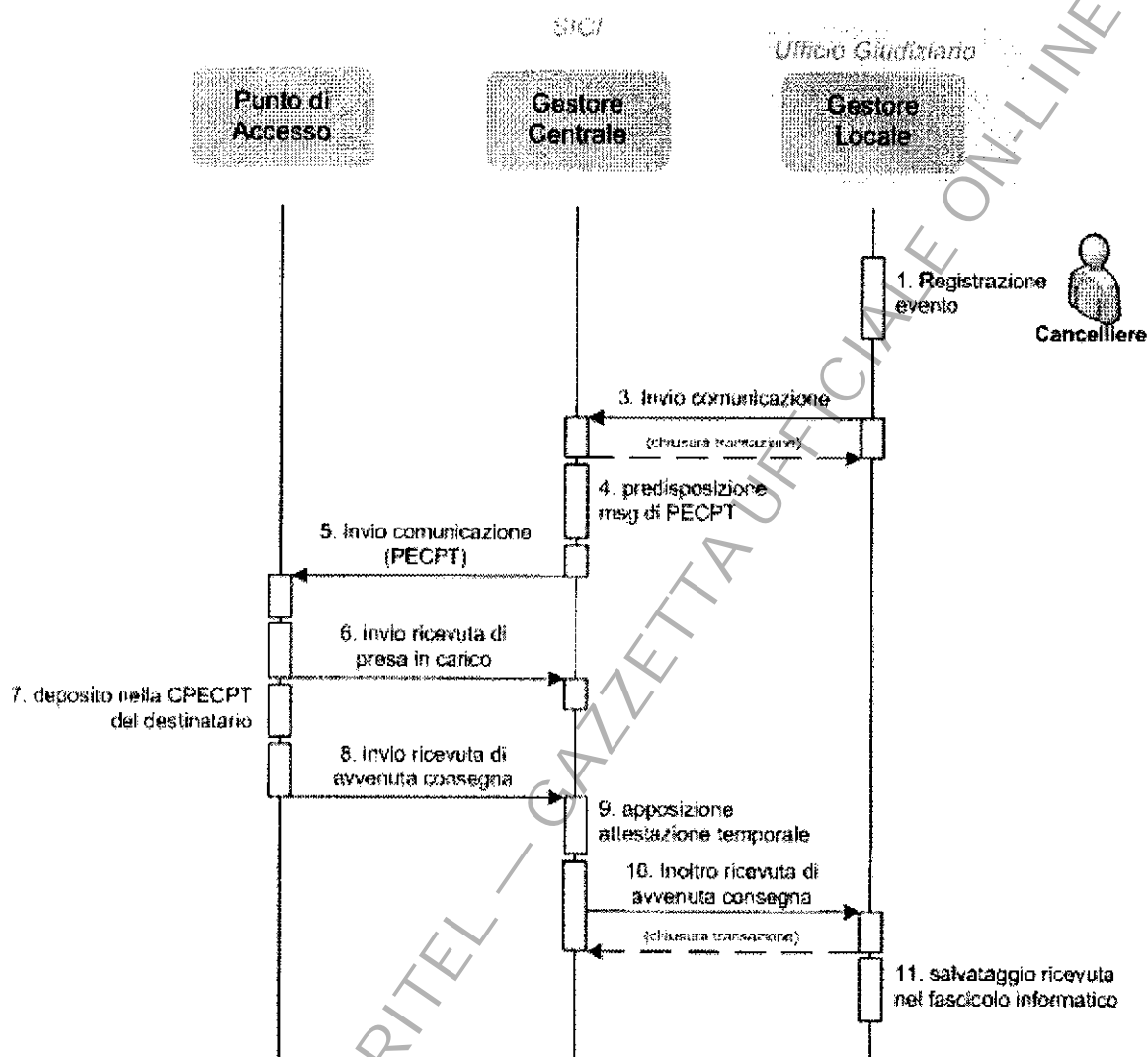
Figura 8 - diagramma di sequenza relativo all'invio della comunicazione di cancelleria

Questa la spiegazione del diagramma sopra riportato.

1. il cancelliere registra l'evento nel sistema di gestione interessato,
2. il quale provvede in automatico a predisporre la comunicazione – in formato XML – e ad aggiornare il fascicolo informatico e il registro di cancelleria;
3. il GL procede quindi ad inviare la comunicazione al GC, nell'ambito di una transazione sincrona;
4. il GC predispone il messaggio di posta elettronica certificata
5. e lo invia alla CPECPT del destinatario presso il suo PdA;
6. il PdA invia la ricevuta di presa in carico al GC;
7. il PdA deposita il messaggio nella CPECPT del destinatario;
8. il PdA invia la ricevuta di avvenuta consegna al GC,

9. il quale appone l'attestazione temporale,
10. e la inoltra al GL, allestendo con esso una transazione sincrona;
11. il GL salva la ricevuta nel fascicolo informatico, rendendo visibili gli estremi al cancelliere nell'ambito del sistema di gestione dei registri interessato.

Ai fini della valutazione di eventuali termini legali per la consegna della comunicazione, fa pertanto fede la data apposta dal GC in fase di attestazione temporale sulla ricevuta di avvenuta consegna prodotta dal PdA.

Il sistema di cancelleria è in grado di gestire le situazioni miste, ossia quando sono previsti sia invii telematici che stampe cartacee, in funzione dell'esistenza o meno dell'indirizzo elettronico del soggetto destinatario.

La comunicazione di cancelleria è strutturata secondo il formato XML. La strutturazione è molto semplice e si limita di fatto ad identificare:

- l'oggetto della comunicazione
- il contenuto della stessa
- il riferimento al fascicolo di cui fa parte.

Il sistema di cancelleria identifica ogni comunicazione con un identificatore univoco che permetterà di legare la comunicazione stessa alla ricevuta di deposito restituita dal GC. Il fascicolo informatico tiene infatti traccia di ogni comunicazione inviata e della relativa ricevuta di consegna.

È compito del PdA presentare al soggetto abilitato i messaggi di risposta ricevuti.

1.3.4 Consultazione web (Polis Web)

La consultazione web riguarda l'accesso alle informazioni di pertinenza contenute nei sistemi di gestione dei registri e nel fascicolo informatico.

L'architettura del sistema aderisce al modello MVC[5], e prevede pertanto il disaccoppiamento del *front-end*, localizzato sul punto di accesso, dal *back-end*, localizzato sul gestore locale, incaricato di esporre i servizi sottoforma di web services.

[5] Model View Controller

L'architettura è schematizzata nella seguente figura:
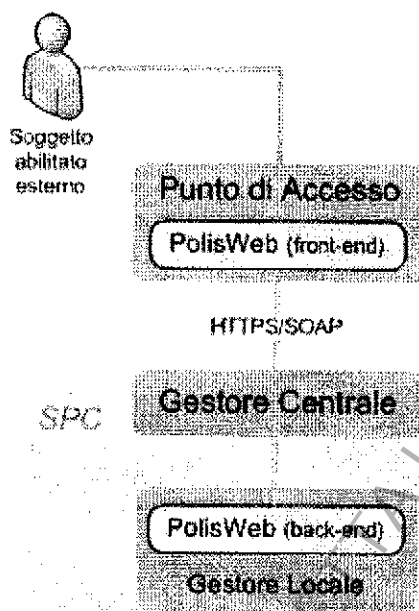
Figura 9 - Architettura di Polis Web

Il flusso tra front-end e back-end è sincrono, con il Gestore Centrale che funge da proxy.

In particolare sono svolte le seguenti azioni:

- Il soggetto abilitato esterno sottopone a Polis Web, presente sul PdA, una richiesta di consultazione;
- Il PdA autentica l'utente, se questi non è già stato precedentemente autenticato, e inoltra la richiesta all'Ufficio Giudiziario, per il tramite del Gestore Centrale;
- Un apposito sottosistema, all'interno dell'UG, predispone le informazioni ottenute a seguito dell'interrogazione del sistema di registro interessato e del sottosistema di gestione del fascicolo informatico (repository documentale) e le inoltra al PdA, per il tramite del GC;
- Polis Web presenta le informazioni in consultazione al soggetto abilitato esterno.

Il punto di accesso è tenuto ad esporre i servizi di consultazione web (web services) esposti dal gestore locale, a beneficio dei soggetti abilitati esterni; questo al fine di consentire ai software gestionali di studio di recuperare direttamente le informazioni dagli uffici giudiziari.

La realizzazione del front-end di Polis Web rimane a cura del Punto di Accesso, trattandosi di un modulo software integrato nel sistema PdA.

1.3.5 Richieste di copie

Nell'ambito del processo civile telematico, il soggetto abilitato esterno può richiedere:

1) Copie digitali semplici: copia elettronica dell'atto in formato elettronico.

2) Copie digitali semplici per l'avvocato non costituito: su richiesta da parte del soggetto, che allega il mandato della parte.
3) Copie digitali autentiche: il sistema di cancelleria, con l'ausilio dell'operatore, effettua il calcolo della quota che il richiedente è tenuto a versare come diritto di cancelleria; il richiedente, dopo aver provveduto al pagamento, compila un'apposita form disponibile su Polis Web, che lega gli estremi di pagamento presenti sulla ricevuta dello stesso all'identificatore della richiesta; a questo punto l'operatore di cancelleria dovrà predisporre il pacchetto di file contenente le copie autentiche controfirmando digitalmente ogni atto/documento richiesto. Nel caso in cui la copia autentica richiesta non possa essere emessa (ad esempio nel caso di un titolo esecutivo già rilasciato) il sistema, automaticamente notificherà al richiedente, a mezzo di comunicazione di cancelleria, l'impossibilità di evadere la richiesta.
4) Copie cartacee semplici: a seguito della richiesta pervenuta, l'operatore di cancelleria invia al richiedente una comunicazione contenente data e ora in cui sarà possibile ritirare i documenti e l'importo da pagare.
5) Copie cartacee autentiche: come il punto precedente, con il più il controllo da parte del sistema per verificare se le copie richieste sono effettivamente rilasciabili. Se l'originale è digitale, il cancelliere attesterà la conformità della versione cartacea, stampata, all'originale digitale apponendo sul cartaceo la propria firma. Al momento del ritiro il richiedente provvederà al pagamento secondo le modalità ad oggi previste.

Le richieste vengono compilate sul punto di accesso ed inviate telematicamente all'ufficio giudiziario, tramite la relativa funzionalità di Polis Web.

Le eventuali copie elettroniche vengono ricevute nella CPECPT del richiedente.

1.3.6 Notifiche tra difensori

La notificazione telematica di documenti informatici tra difensori consiste nell'inoltro del documento dal Punto di Accesso del mittente alla CPECPT del destinatario.

A tale scopo il PdA deve trasmettere il messaggio con il documento da notificare al Gestore Centrale che, a sua volta, inoltra il messaggio ricevuto al Punto di Accesso di destinazione.

In figura il diagramma di sequenza relativo.
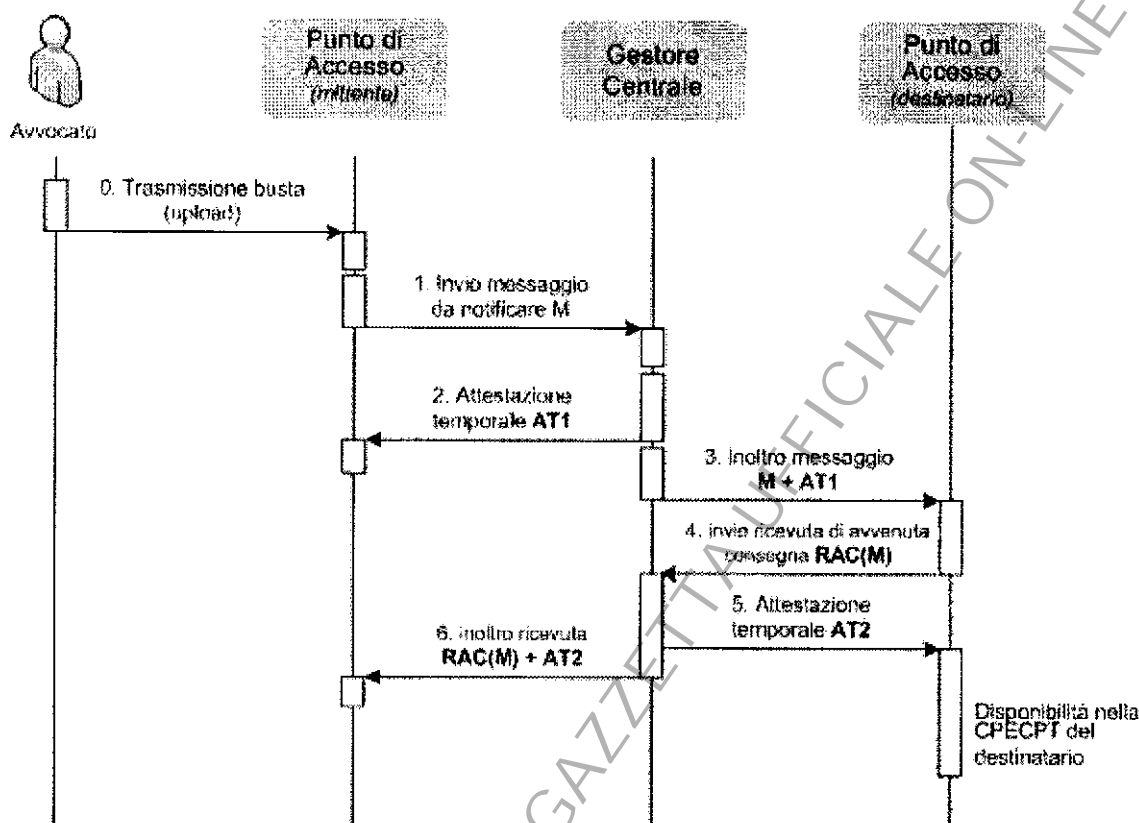
Figura 10 – Diagramma di sequenza notifiche tra difensori (avvocato-avvocato)

Di seguito viene descritto il flusso organizzativo illustrato nel diagramma di sequenza, per quanto di competenza del Punto di Accesso:

0. l'avvocato predispone la busta contenente la comunicazione, che viene firmata digitalmente e, se necessario, anche cifrata con la chiave pubblica dell'avvocato destinatario. La busta comprende anche le indicazioni di routing del messaggio in chiaro, in modo analogo a come avviene per l'inoltro atto, all'interno del file *InfoNotifica.xml*; l'avvocato si autentica sul proprio PdA, effettua l'upload della busta e seleziona la funzionalità di invio comunicazione ad avvocato;
1. il PdA effettua i controlli necessari, completa il file XML contenente le informazioni di instradamento del messaggio ed invia la busta al GC;
2. se corretta il GC appone l'Attestazione Temporale (AT1) alla comunicazione, e la indirizza alla CPECPT dell'avvocato mittente e
3. insieme al messaggio (M + AT1), alla CPECPT dell'avvocato destinatario;
4. la CPECT del destinatario, ricevuto il messaggio, invia al Gestore Centrale dell'accesso la ricevuta di avvenuta consegna RAC(M);
5. all'atto della ricezione della ricevuta di avvenuta consegna da parte del PdA dell'avvocato destinatario, il GC esegue una nuova attestazione temporale (AT2), che viene inviata alla CPECPT dell'avvocato destinatario e

6. insieme alla RAC, inserita in un messaggio indirizzato alla CPECPT dell'avvocato mittente: RAC(M) + AT2.

Non è previsto l'invio di una notifica a più di un destinatario o a liste di destinatari.

Per inviare comunicazioni e notifiche ad altri avvocati, ciascun avvocato deve conoscerne il codice fiscale e, qualora la comunicazione debba essere cifrata, deve avere a disposizione sul proprio posto di lavoro la chiave pubblica di cifratura del destinatario. Tali informazioni sono reperibili tramite un servizio di accesso LDAP per l'interrogazione del Registro degli Indirizzi Elettronici sul Gestore Centrale, come descritto in 2.12.1.

2 DETTAGLI TECNICI

I DTD relativi agli allegati xml nonché gli schemi dei messaggi previsti nelle comunicazioni tra GC e PdA sono pubblicati nel decreto di cui all'art. 62, comma 2.

In corrispondenza di ogni tipologia di messaggio (e relativo schema) sono previsti uno o più tipi di buste che riflettono la struttura del messaggio stesso ma che si differenziano per il contenuto del subject.

2.1 FLUSSO DI ABILITAZIONE E GESTIONE UTENZE

Lo scambio di messaggi tra PdA, GC e CdO dei flussi di gestione utenze (iscrizione, variazione dati, cancellazione, invio albo, variazione status) avviene per via telematica, tramite PECPT, e le comunicazioni sono strutturate in linguaggio XML, secondo il formato definito nel relativo decreto di cui all'art. 62, comma 2.

La casella di PECPT del GC a cui inviare questi messaggi è la seguente: gestorecentrale@giustiziacertpt.it.

Ai fini dell'invio, ogni Consiglio dell'Ordine possiede una CPECPT, anche in caso che questa sia gestita su delega; l'indirizzo di tale casella è conforme alla seguente sintassi: <codiceOrdine>@<dominioPECPT.it>.

Per lo scambio dei dati relativi alla gestione delle utenze viene utilizzata la struttura di *ComunicazioneIndirizzi.xml*

In particolare, nella struttura *ComunicazioneIndirizzi.xml*, l'elemento "TipoOperazione" indica la tipologia di operazione, secondo il seguente formalismo:

"I": operazione di iscrizione di una nuova utenza inviata dal PdA

"M": operazione di variazione dei dati generata dall'utente stesso

"V": richiesta di variazione dello status professionale o di iscrizione di un nuovo avvocato, generata dal CdO

"C": richiesta di cancellazione, inviata da PdA o da CdO

2.1.1 Messaggi utilizzati nei flussi di variazione utenze

Di seguito un elenco dei messaggi utilizzati nei flussi di gestione utenze la cui struttura è documentata nel decreto di cui all'art. 62, comma 2:

- *RichiestaAggiornamentoUtenze:* viene inviato dal Pda al GC per le operazioni di iscrizione, cancellazione o variazione dati generate dall'utente stesso.
- *AggiornamentoUtenze*: viene inviato dal rappresentante del CdO o dal CNF e può contenere la copia dell'albo dell'Ordine in formato elettronico oppure una variazione dello stato professionale di uno o più avvocati. Il messaggio contiene l'allegato *ComunicazioneIndirizz.xml* sottoscritto con firma digitale.

- *AttestazioneCertificata, EccezioneCertificata:* effettuati i controlli formali su pacchetti di richiesta di aggiornamento utenze, inviati da PdA o da CdO o CNF, il Gestore Centrale invia in caso di esito positivo un messaggio di *AttestazioneCertificata* o un messaggio di *EccezioneCertificata* in caso di esito negativo.
- *ComunicazioneIndirizzi, AnomaliaIndirizzi*: il Gestore Centrale, un volta controllato il merito delle richiesta (*AggiornamentoUtenze* o *RichiestaAggiornamentoUtenze*) in caso positivo effettua l'aggiornamento del ReGIndE ed invia al mittente un messaggio *ComunicazioneIndirizzi* di conferma. In caso di esito negativo dei controlli il GC invia un messaggio di *AnomaliaIndirizzi* contenente indicazioni sulle anomalie riscontrate (utilizzando il campo "*Eccezione*" dell'allegato *ComunicazioneIndirizzi.xml).*
- Il GC, ad ogni richiesta di aggiornamento ricevuta dal PdA, e correttamente elaborata, inoltra al CdO di competenza un messaggio di *RichiestaAggiornamentoUtenze* come notifica dell'aggiornamento sopravvenuto.
- Il GC, ad ogni richiesta di aggiornamento ricevuta dal CdO, e correttamente elaborata, inoltra al PdA di competenza un messaggio di *AggiornamentoUtenze* come notifica dell'aggiornamento sopravvenuto.

2.2 CIFRATURA E FIRMA DELL'ATTO DI PARTE

La modalità di apposizione della firma denominata **firme indipendenti (meccanismo "aggiungi una firma")**, prevede che uno o più soggetti firmino digitalmente lo stesso documento. L'ordine di apposizione delle firme degli N firmatari non è significativo, ed il file generato si presenta con un'unica estensione *p7m*.

La struttura è quindi PKCS#7 in cui sono contenute le N firme che si riferiscono quindi, al medesimo documento. Non è possibile utilizzare tale meccanismo per stabilire l'ordine in cui le firme stesse sono state apposte: una alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica PKCS#7.

Tale meccanismo è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

In Figura 11 è rappresentata la struttura PKCS#7 del file firmato.
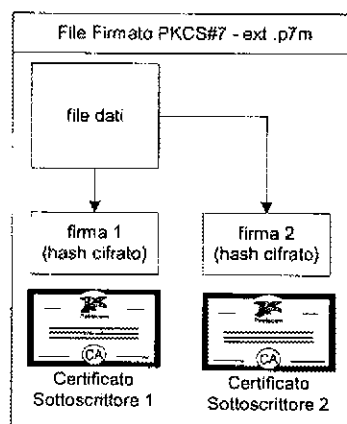
Figura 11 – Struttura del file firmato

Tali oggetti, creati sulla postazione dell'avvocato, vengono aggregati, ai fini del deposito, in un'opportuna struttura dati denominata "busta MIME" che contiene le informazioni di instradamento, i riferimenti ai documenti atto ed allegati, l'atto firmato (*corpoatto.xml.p7m*) e gli eventuali allegati (nella figura che segue l'allegato è *AllegatoX.pdf.p7m*) .

Di seguito viene rappresentata la struttura dell'oggetto MIME, di cui è fornito apposito DTD.
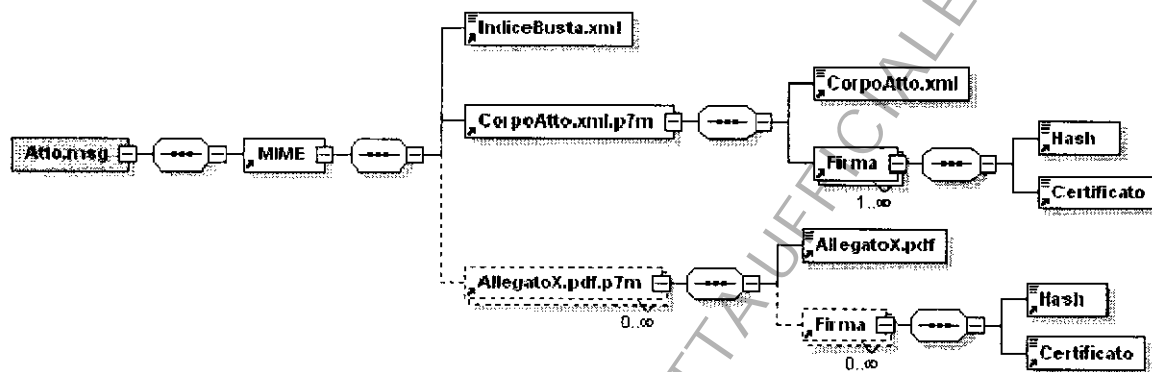
Figura 12 - Struttura MIME contenente l'atto i suoi allegati e l'indice degli stessi

La busta così composta è successivamente cifrata per l'ufficio giudiziario di destinazione, in modo che soltanto questo ufficio possa decifrarlo e quindi leggere il contenuto della busta.

Lo standard previsto è il PKCS #7.

Atto.msg è l'atto cifrato con chiave di sessione. *ChiaveSessione* è la chiave di sessione cifrata con il certificato del destinatario. *IssuerDname* è il *Distinguished Name* della CA che ha emesso il certificato dell'ufficio giudiziario destinatario, *SerialNumber* è il numero seriale del certificato dell'ufficio giudiziario destinatario. Tali dati sono necessari per il controllo successivo in fase di decifratura ed identificano il certificato con cui è stato cifrato l'oggetto.

Di seguito viene rappresentato lo schema della busta ottenuta a seguito del processo di cifratura dell'oggetto MIME contenuto nell'oggetto *Atto.msg*.
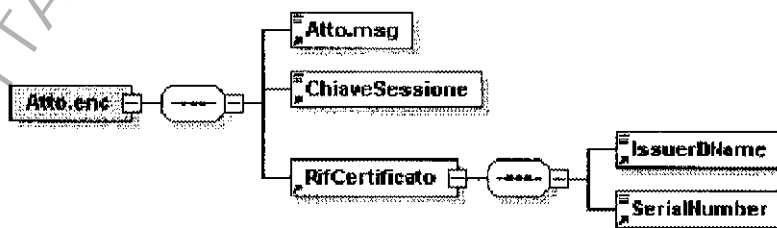
Figura 13 - Schema del risultato dell'operazione di cifratura di Atto.msg

L'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione vengono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario con il quale si intende corrispondere.

Tale busta sarà successivamente depositata presso l'Ufficio Giudiziario per il tramite del Punto di Accesso e del Gestore Centrale.

2.3 TRASMISSIONE DELL'ATTO

I messaggi SMTP relativi alla funzione di *deposito atto*, coinvolgono i seguenti due indirizzi:

Gestore Centrale: **gestorecentrale@processotelematico.giustizia.it**

Punto di Accesso: **<codicePdA>@<dominioPdA>**.

I messaggi interessati (la cui struttura è documentata nel decreto di cui all'art. 62, comma 2) sono:

- *InoltroAtto*: il messaggio di inoltro della busta trasmessa dal PdA al GC, contenente *Atto.enc* e *InfoInoltro.xml*;
- *AttestazioneTemporale*: il messaggio contenente l'attestazione temporale inviato dal GC al PdA (vedi paragrafo 2.3.3);
- *NotificaEccezione*: il messaggio di notifica eccezione inviato dal GC al PdA alternativo all'attestazione temporale (vedi paragrafo 2.3.4);
- *EsitoAtto*: i messaggi di esito deposito inviati dal GC al PdA contenenti l'esito del deposito lato UG (vedi paragrafo 2.4). In questo caso si hanno due tipi di esito: uno inviato a seguito dei controlli automatici da parte del GL e l'altro a seguito dell'intervento da parte del Cancelliere.

I messaggi ricevuti dal GC hanno una testata SMTP standard in cui viene richiesto di impostare almeno i parametri "MSG-ID" e "FROM" (da utilizzare per individuare la provenienza del messaggio quando non è possibile procedere all'apertura della busta ricevuta).

I messaggi inviati dal GC al PdA hanno una testata SMTP standard in cui il subject è definito in base al tipo di messaggio (il formato dei subject è specificato nel decreto di cui all'art. 62, comma 2).

Il GC svolge una funzione di garante del processo di inoltro assicurando che gli atti informatici depositati presso i GL non contengano errori attribuibili alle attività svolte dai PdA, ma solo eventualmente ascrivibili ad operazioni svolte in locale dall'Avvocato in fase di formazione dell'atto informatico, tenendo comunque conto che l'atto ed i suoi allegati sono criptati (in *Atto.enc*).

Nel seguito viene descritta la struttura applicativa di ciascun messaggio generato nella fase di trasmissione dell'atto.

2.3.1 Struttura del messaggio di "inoltro atto"

La struttura del messaggio SMTP di *Inoltroatto* è costituita da un S/MIME, cioè da una struttura MIME sottoscritta da parte del PdA con proprio certificato server, a titolo di verifica della integrità del messaggio.

Pertanto al suo interno è riconoscibile:

- una struttura MIME;
- l'hash del MIME, cioè la registrazione in formato binario che contiene l'impronta del documento, firmata secondo le modalità tecniche previste dal D.P.R. 513/97 e dalle relative regole tecniche (D.P.C.M. 8/02/99).
- il Certificato del PdA, ossia una struttura dati tipo X.509. I dati forniscono informazioni sul possessore del certificato, il firmatario del certificato, la versione, il numero seriale, l'algoritmo di firma, il periodo di validità, la corrispondente chiave pubblica e altri dati.

Le parti costituenti la struttura MIME sono:

- File **InfoInoltro.xml**: contiene le informazioni di servizio per il GC. Tali informazioni consentono il routing del messaggio e la verifica dei dati di certificazione.
- File **Atto.enc**: è l'atto informatico prodotto dall'Avvocato, criptato utilizzando la chiave pubblica di cifratura dell'UG destinatario.
- File **Certificazione.xml.p7m:** può mancare nella busta di *InoltroAtto* se il PdA non dispone delle informazioni atte a certificare l'Avvocato.

2.3.2 Struttura del messaggio di "deposito atto"

La busta di *DepositoAtto* presenta la struttura appresso schematizzata:
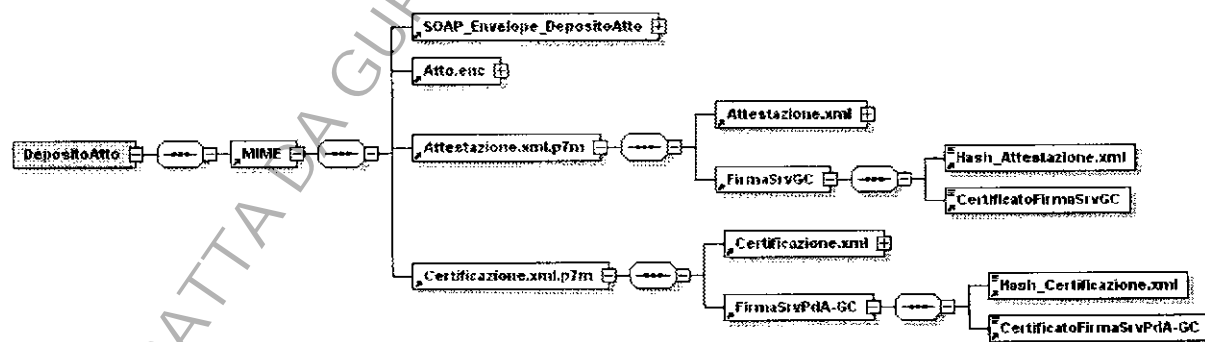
Figura 14 – MIME di Deposito Atto

dove la struttura SOAP_Envelope_DepositoAtto ha la seguente rappresentazione grafica:
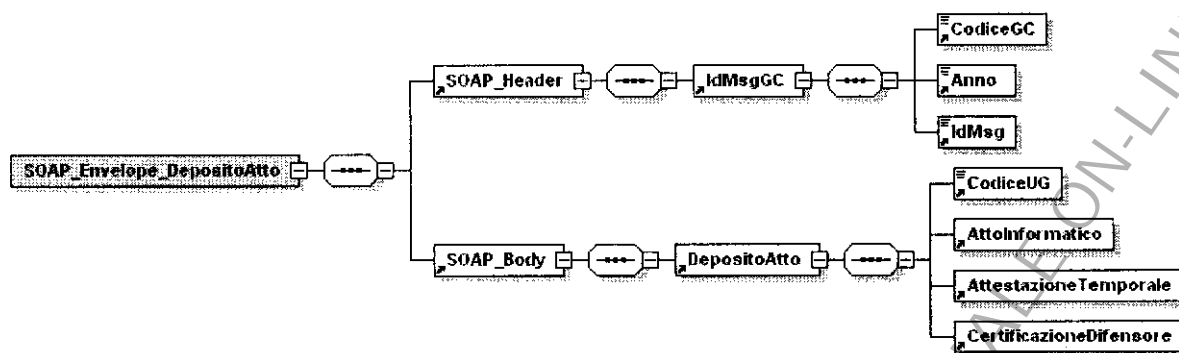
Figura 15 – Struttura SOAP_Envelope di DepositoAtto

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioDepositoAtto>.

La busta *DepositoAtto* contiene le seguenti strutture:

1. SOAP:Envelope

La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto (in questo caso il messaggio di *Inoltroatto*).

Il body della struttura ha un elemento, denominato *DepositoAtto* contenente:

CodiceUG	=	E' il codice dell'UG cui è destinato l'Atto informatico, ricavato da *InfoInoltro/Destinatario/CodiceUG*
Atto	=	Referenzia l'Atto informatico (file Atto.enc), generato dall'Avvocato, allegato nel MIME.
AttestazioneTemporale	=	Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME.
CertificazioneDifensore	=	Referenzia il file Certificazione.xml.p7m, ricevuto dal PdA o generato e firmato dal GC, allegato nel MIME.

2. File Atto.enc

Si veda il paragrafo 2.3.1.

3. File Attestazione.xml.p7m

All'atto della ricezione di un messaggio di *InoltroAtto* da parte del PdA, e dopo averne verificato la correttezza, il GC esegue l'attestazione temporale dell'evento di ricezione della richiesta di inoltro dell'atto. L'attestazione temporale si sostanzia nella generazione del file *Attestazione.xml.*

4. File Certificazione.xml.p7m

Il file Certificazione.xml.p7m è lo stesso presente nella busta di *InoltroAtto.* Qualora tuttavia il PdA non disponesse delle informazioni atte a certificare l'Avvocato, il GC deve eseguire la certificazione sostitutiva e sottoscrivere il file con la propria firma digitale (firma server).

2.3.3 Il messaggio di risposta "attestazione temporale"

Oltre al deposito dell'atto presso il GL destinatario, il GC genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto, un messaggio di *AttestazioneTemporale*.

Il messaggio contiene allegato all'interno della struttura MIME lo stesso file *Attestazione.xml.p7m* trasmesso all'UG.

2.3.4 Il messaggio di risposta "notifica eccezione"

Qualora il GC riscontri un errore nella formazione della busta di *InoltroAtto*, oltre a non eseguire il deposito dell'atto, genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto un messaggio di *NotificaEccezione*, contenente in allegato *Eccezione.xml*.

2.4 RICEZIONE E ACCETTAZIONE DELL'ATTO DI PARTE

In fase di accettazione il Gestore Locale opera i controlli attraverso la componente applicativa denominata ***Log Eventi***.

Il log eventi è un'insieme persistente di informazioni che permettono di tracciare **tutte le operazioni** che, sia le componenti applicative sia gli operatori di cancelleria, effettuano sugli atti in ingresso all'UG. A tal fine il sistema registra la tipologia di operazione che il sistema o l'operatore esegue (in forma codificata), la descrizione di tale operazione, il riferimento al documento (atto o allegato) oggetto dell'operazione e l'indicazione temporale del momento in cui viene eseguita.

Il Gestore Locale si compone dei seguenti sistemi:

Il **sistema di ricezione** è l'interfaccia esposta dall'UG verso il GC e si occupa esclusivamente di ricevere attraverso una comunicazione sincrona l'atto giudiziario e i suoi allegati in una busta cifrata con chiave pubblica dell'UG. Il componente si occupa di gestire attraverso meccanismi tipici del protocollo di comunicazione (HTTP) eventuali problemi trasmissione a meno dei quali la busta viene memorizzata localmente in un'area del Repository Documentale denominata *Area Buste*. La memorizzazione nell'area buste garantisce sicurezza dell'avvenuta ricezione di una busta integra in tutte le sue componenti ovvero informazioni sul mittente, attestazione temporale e pacchetto dati cifrato contenente l'atto giudiziario e i suoi eventuali allegati.

Il **sistema dei controlli** è una componente altamente configurabile che permette di individuare eventuali errori bloccanti o semplici anomalie sull'atto depositato e comunicare le stesse all'operatore di cancelleria attraverso il log eventi. È stato realizzato un vero e proprio sistema di *ruling* altamente personalizzabile con l'obiettivo di conferire al sistema un alto grado di flessibilità ed elasticità necessario soprattutto nella fase sperimentazione.

Il **sistema di accettazione** è in grado di utilizzare il motore stati eventi per lo scarico dell'evento corrispondente al deposito dell'atto e di memorizzare l'atto stesso nel fascicolo elettronico attraverso l'interfacciamento con il repository documentale. Il sistema di accettazione viene attivato solo nel caso in cui tutti i controlli diano esito positivo.

Il **fascicolo elettronico** indica quell'area del repository documentale utilizzata per la memorizzazione degli atti di parte e d'ufficio e dei relativi allegati.

Il **sistema di diagnostica** è utilizzato dagli amministratori di sistema dell'UG per individuare e intervenire a livello esclusivamente tecnico sull'atto pervenuto all'UG. Il sistema di diagnostica fornisce agli amministratori un'interfaccia attraverso la quale registrate gli interventi nel log eventi.

Il **sistema per la consultazione del log eventi** mette a disposizione degli operatori di cancelleria un'interfaccia grafica potente e flessibile che permette loro di verificare tutte le operazioni effettuate dal sistema in automatico. Nel caso di errori o anomalie tale interfaccia permette in maniera semplice di intervenire manualmente, laddove possibile, per riuscire comunque ad aggiornare il SICC e il fascicolo elettronico.

2.5 GESTIONE DEL FASCICOLO INFORMATICO

Il Repository Documentale nasce per gestire il fascicolo informatico, conservare i documenti prodotti nell'ambito di un procedimento giudiziario ed esporre ai sistemi utilizzatori servizi informatici di alimentazione e fruizione delle informazioni.

Tale servizio si configura come una piattaforma di gestione documentale che mette in comunicazione i diversi applicativi con la base dati documentale, per consentire l'interazione documentale ed informativa fra soggetti appartenenti a categorie diverse tra loro (Giudice, Cancelliere, Avvocato, CTU).

L'obiettivo principale del Repository Documentale è quello di potenziare le funzionalità delle Applicazioni di Gestione dei Registri, con capacità di Gestione Documentale ed *Information Retrieval*, fornendo in sintesi i seguenti servizi:

- acquisizione dei documenti contenuti nelle Buste ricevute;
- acquisizione delle comunicazioni inviate dalla Cancelleria dell'Ufficio Giudiziario verso l'esterno;
- consultazione di documenti.

Il Repository Documentale funge pertanto da gestore centralizzato del patrimonio documentale, divenendo l'unità di archiviazione univoca e centrale a livello di UG dei documenti prodotti o ricevuti dall'Ufficio stesso, indipendentemente dalla loro natura originaria, analogica o digitale.

L'accessibilità agli oggetti documentali gestiti dal Repository è demandata ai sistemi di gestione dei registri di cancelleria.

2.6 TRASMISSIONE DELL'ESITO DELL'ATTO

2.6.1 Struttura del messaggio di esito atto

Il GL, in risposta alla ricezione di un atto informatico, genera e inoltra al GC due messaggi di esito: un primo esito automatico e un secondo esito a seguito dell'intervento di accettazione (o rifiuto) da parte del cancelliere.

La busta MIME relativa all'esito è così schematizzata:
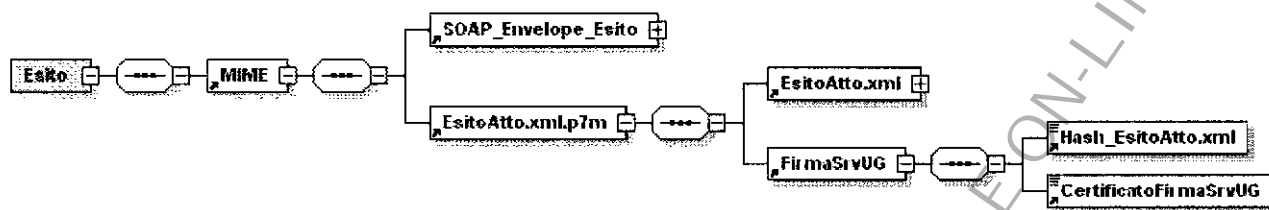
Figura 16 – MIME di Esito

dove la struttura SOAP_Envelope_Esito ha la seguente rappresentazione grafica:
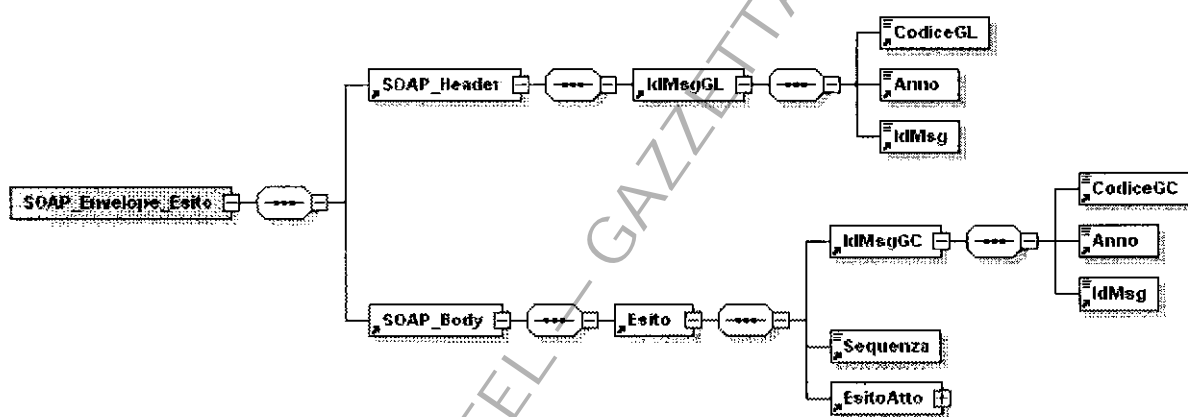
Figura 17 – Struttura SOAP_Envelope di Esito

Il messaggio viene ricevuto dal GC all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/PTRicezione.asp.

1. SOAP:Envelope della busta di Esito

La struttura contiene a livello di header l'identificativo univoco del messaggio di *Esito* generato dal GL.

Il body della struttura ha un elemento, denominato Esito, contenente:

IdMsgGC	=	È l'identificativo univoco del messaggio di *Deposito atto* generato dal GC.
EsitoAtto	=	Referenzia il file EsitoAtto.xml.p7m allegato nel MIME.
Sequenza	=	Indica se il messaggio di esito è relativo ai controlli automatici (1) o all'intervento del cancelliere (2)

2. File EsitoAtto.xml.p7m

Il file *EsitoAtto.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni che comunicano all'Avvocato l'esito dell'atto.

Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti.

Le due tipologie di esito previste sono differenziate in base al subject della busta.

2.6.2 Il messaggio di risposta "comunicazione esito"

Quando il GC riceve un messaggio di *EsitoAtto*, attraverso l'identificativo del messaggio (*IdMsgGC*) ricava tutte le informazioni necessarie per recapitare il messaggio *ComunicazioneEsito* all'Avvocato destinatario sul PdA di appartenenza.

Il messaggio contiene allegato all'interno della struttura MIME il file EsitoAtto.xml.p7m firmato dall'UG.

2.7 CIFRATURA DEGLI ATTI IN USCITA DALL'UFFICIO GIUDIZIARIO

Relativamente alla cifratura degli atti in uscita, ossia cifrati a cura del GL con la chiave pubblica del soggetto abilitato esterno (disponibile sul registro generale degli indirizzi presso il gestore centrale), quando questa verrà prevista, si applicheranno le stesse specifiche riportate al paragrafo 2.2.

In particolare, per gli atti inviati alla casella di posta certificata del destinatario, verrà utilizzata la medesima struttura di *atto.enc*, che verrà allegato al messaggio di posta elettronica certificata.

Ai fini della consultazione web degli atti, sarà valido quanto segue:

- il GL prepara la risposta SOAP alla richiesta di consultazione e inserisce all'interno di questa un "blob" (in codifica base64) che a sua volta contiene:
    - L'XML dell'atto richiesto, cifrato con crittografia simmetrica utilizzando l'algoritmo 3-DES e chiave di sessione;
    - la chiave di sessione cifrata con la chiave pubblica del certificato di cifratura dell'Avvocato;
    - il certificato utilizzato per la cifratura.
- Il Front-End di Polis Web riceve la risposta SOAP, estrae il "blob" e prepara la risposta HTML inserendo all'interno di essa il "blob".

2.8 COMUNICAZIONI DI CANCELLERIA

Il Gestore Centrale gestisce in sostanza le caselle di posta elettronica certificata dei singoli Uffici Giudiziari.

I messaggi di Posta Certificata del Processo Telematico relativi alla funzione di *invio comunicazione di cancelleria* vengono spediti alle CPECPT degli Avvocati agli indirizzi **<CPECPT>@<dominiocertPdA>** e ricevuti sulle CPECPT degli UG presso il GC agli indirizzi **<codiceGL>@giustiziacertpt.it**.

I messaggi prodotti dal GC sono conformi allo standard previsto dal sistema di Posta Certificata.

Nel seguito del documento viene descritta la struttura applicativa di ciascun messaggio generato dalla funzione di invio di un biglietto di cancelleria; i relativi DTD verranno pubblicati nel decreto di cui all'art. 62, comma 2.

2.8.1 Struttura del messaggio di "comunicazione UG"

La struttura del messaggio di *comunicazioneUG* proveniente da un GL è illustrata nella figura che segue:
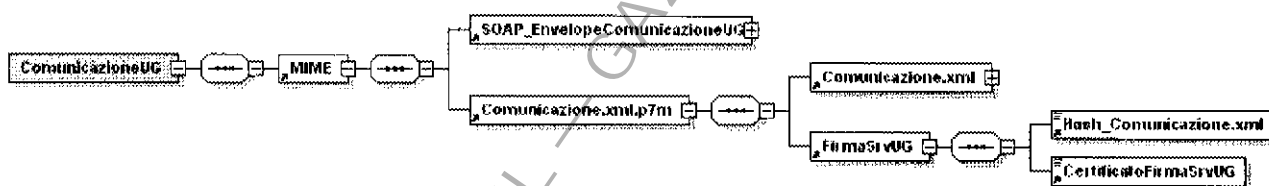
Figura 18 – MIME di Comunicazione UG

dove la struttura SOAP_EnvelopeComunicazioneUG ha la seguente rappresentazione grafica:
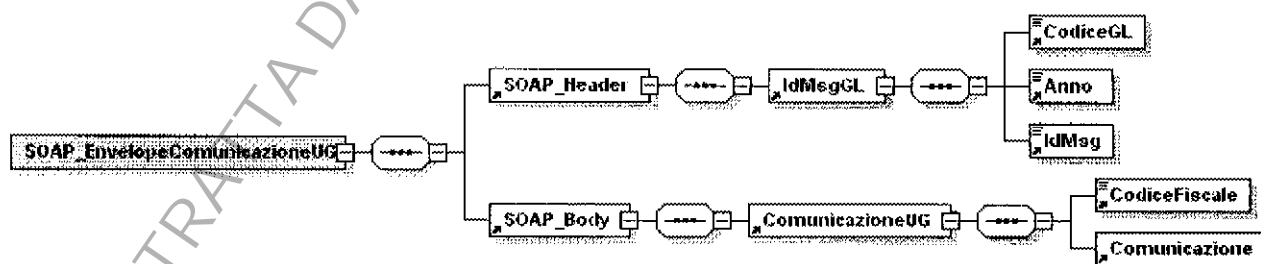
Figura 19 – Struttura SOAP_Envelope di ComunicazioneUG

Il messaggio viene ricevuto dal GC, all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/PTRicezioneComunicazione.asp.

La transazione tra GL e GC termina con successo solo dopo che il GC ha effettuato i controlli formali sulla busta ricevuta ed ha controllato che il codice fiscale del destinatario sia presente nel ReGIndE.

La busta *ComunicazioneUG* contiene le seguenti strutture:

1. **SOAP:Envelope**

   La struttura contiene a livello di header l'identificativo univoco del messaggio generato dal GL (*IdMsgGL*).

   Il body della struttura ha un elemento, denominato *ComunicazioneUG*, contenente:

   CodiceFiscale = È l'identificativo del destinatario della comunicazione.

   Comunicazione = Referenzia il file Comunicazione.xml.p7m allegato nel MIME.

2. **File Comunicazione.xml.p7m**

   Il file *Comunicazione.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni relative alla comunicazione da trasmettere all'Avvocato.

   Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti, per il cui dettaglio si rimanda al documento di "Analisi funzionale del Processo Telematico".

2.8.2 Struttura del messaggio di "biglietto cancelleria"

Ricevuta la comunicazione da parte del GL, il servizio SMTP del GC genera un messaggio di Posta Certificata del Processo Telematico contenente in allegato il file *Comunicazione.xml.p7m*.

Il messaggio riporta come destinatario la CPECPT dell'Avvocato corrispondente al codice fiscale trasmesso, e come mittente la CPECPT dell'UG dal quale è stata ricevuta la comunicazione.

Tale messaggio, secondo i meccanismi standard di Posta Certificata, viene acquisito dal server di dominio del GC, imbustato in un messaggio di trasporto (*BigliettoCancelleria*) e spedito al server di dominio di Posta Certificata del PdA.

Il messaggio contiene in allegato il file *AttoUG.enc* corrispondente alla comunicazione firmata dall'UG che l'ha generata (*Comunicazione.xml.p7m*), ed il file *InfoIndirizzamento.xml* contenente tutte le informazioni necessarie al routing del messaggio, il numero di ruolo e l'oggetto del biglietto di cancelleria.

A seguito di tali operazioni il server SMTP di Posta Certificata del GC restituisce nella CPECPT dell'UG mittente una *ricevuta di accettazione* che segnala l'effettiva spedizione del messaggio.

2.8.3 Struttura del messaggio di "ricevuta comunicazione"

All'atto della ricezione nella CPECPT dell'UG mittente della *ricevuta di avvenuta consegna* il GC genera automaticamente l'attestazione temporale di tale evento.

Il file Attestazione.xml.p7m insieme con la *ricevuta di avvenuta consegna* viene imbustato in un messaggio di *RicevutaComunicazione* che presenta la struttura appresso schematizzata:
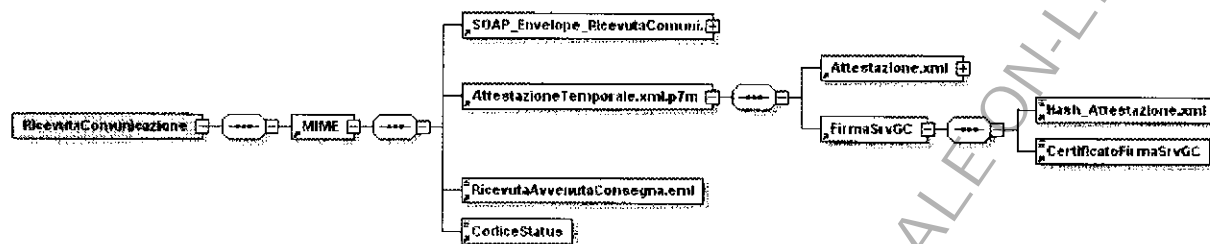
Figura 20 – MIME di Ricevuta comunicazione

dove la struttura SOAP_Envelope_RicevutaComunicazione ha la seguente rappresentazione grafica:
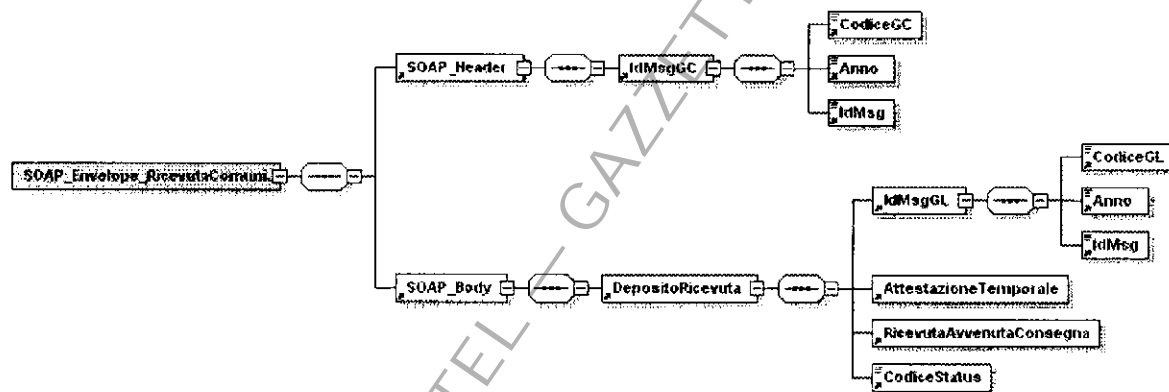
Figura 21 – Struttura SOAP_Envelope di RicevutaComunicazione

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioRicevutaComunicazione>.

La busta *RicevutaComunicazione* contiene le seguenti strutture:

1. SOAP:Envelope

La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto.

Il body della struttura ha un elemento, denominato *DepositoRicevuta* contenente:

IdMsgGL	=	E' l'identificativo della comunicazione trasmessa dall'UG.
AttestazioneTemporale	=	Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME.
RicevutaAvvenutaConsegna	=	Referenzia il file RicevutaAvvenutaConsegna.eml ricevuto dal PdA, allegato nel MIME.

CodiceStatus	=	Contiene il codice dello status professionale dell'Avvocato destinatario della comunicazione (attivo, sospeso, radiato).

2. File Attestazione.xml.p7m

Il file Attestazione.xml.p7m è firmato dal GC (firma server). Il contenuto informativo di tale file è il seguente:

- IdMsgSMTP.

IdMsgSMTP	=	Contiene il valore del parametro SMTP Message-ID del messaggio di *ricevuta di avvenuta consegna*

- IdMsgMitt e IdMsgPdA.

  In questo caso non sono valorizzati (questi elementi sono alternativi rispetto al precedente).

- DatiAttestazione.

DatiAttestazione	=	Contiene l'impronta della busta di *ricevuta avvenuta consegna* (nel formato S/MIME) e la data e ora dell'evento di attestazione temporale

3. File RicevutaAvvenutaConsegna.eml

E' il messaggio di *ricevuta di avvenuta consegna* così come ricevuta dal dominio di Posta Certificata del Processo Telematico del PdA.

2.9 CONSULTAZIONE WEB (POLIS WEB)

Il Punto di Accesso deve mettere a disposizione il front-end di Polis Web, realizzato in autonomia, fermo restando i requisiti di sicurezza di cui al paragrafo 2.9.1.

Ogni funzionalità di consultazione è di tipo sincrono e prevede un flusso che si scompone in:

- flusso di richiesta verso il gestore locale (Ufficio Giudiziario);
- flusso di risposta dal gestore locale (Ufficio Giudiziario).

Il flusso di consultazione è sempre attivato dall'utente (soggetto abilitato esterno) che invia la propria richiesta all'Ufficio Giudiziario, tramite il sistema front-end di PolisWeb fornito dal PdA, transitando per il Gestore Centrale.

All'interno dell'UG il sottosistema Gestore Locale predispone le informazioni ottenute a seguito dell'interrogazione del SICI e del sottosistema di gestione del fascicolo informatico (repository documentale) e le inoltra al PolisWeb, per il tramite del GC.

Il Gestore Locale implementa i propri servizi di consultazione attraverso dei Web Service e PolisWeb interagisce con essi utilizzando il protocollo di trasporto **HTTPS** e la serializzazione dei messaggi nel formato **XML/SOAP**.

Le funzionalità fornite dai Web Service realizzati, nonchè le relative regole di invocazione vengono descritte tramite **WSDL**, pubblicati nel decreto di cui all'art. 62, comma 2.

Nel colloquio tra il Punto di Accesso e PolisWeb si evidenziano le seguenti esigenze:

- Attivazione di una sessione utente di PolisWeb.
- Richiesta di Consultazione Informazioni di PolisWeb.
- Chiusura di una sessione utente di PolisWeb.
- Gestione delle eccezioni.

A seguito dell'autenticazione sul PdA, un utente può quindi effettuare la richiesta di una funzione di consultazione fornita dal front-end PolisWeb del Punto di Accesso:

- La richiesta da parte dell'utente di attivazione di una funzione di consultazione viene inoltrata al Front-End di PolisWeb. PolisWeb fornisce la funzione richiesta per consentire all'utente di indicare i parametri necessari alla ricerca delle informazioni a lui utili.
- I parametri di ricerca forniti dall'utente possono essere ad esempio relativi ad una ricerca di consultazione di informazioni del Contenzioso Civile, fornite dall'Ufficio Giudiziario specifico. I parametri sono inoltrati dal Punto di Accesso al Front-End di PolisWeb.
- Il Front-End di PolisWeb, in base ai parametri ricevuti, prepara il messaggio di richiesta (XMLSoap) da indirizzare al Gestore Centrale per l'inoltro all'Ufficio Giudiziario indicato dall'utente.

- La richiesta di informazioni ricevuta dal Back-End di PolisWeb presso l'Ufficio Giudiziario (Servizi Soap dell'Application Server Comune) viene elaborata con l'interrogazione della base dati di interesse (es. Contenzioso Civile e/o Fascicolo Elettronico).
- Le informazioni così individuate, sono fornite in risposta al Gestore Centrale per l'inoltro al Front-End di PolisWeb presso il Punto di Accesso richiedente.
- L'Utente può consultare le informazioni di risposta, in base ai parametri di ricerca precedentemente forniti.

2.9.1 Requisiti di sicurezza

Si elencano di seguito i requisiti di sicurezza del Front-end di PolisWeb.

- Il sottosistema PolisWeb deve essere localizzato all'interno della Intranet del Punto di Accesso e non deve essere accessibile direttamente dall'esterno (Internet, Interdominio, altro).
- Il sottosistema PolisWeb deve risiedere in un'area privata del PdA a cui l'utente deve accedere tramite autenticazione con certificato digitale (Smart-Card).
- L'applicazione PolisWeb per l'individuazione delle informazioni di visualizzazione sul Front-End, deve interfacciarsi al GC per accedere ai servizi di back-end esposti dai GL.
- Le comunicazioni con il GC devono essere basate su protocollo HTTPS/SOAP su SSL con autenticazione client per lo scambio delle informazioni.
- Il Front-End di PolisWeb deve essere configurabile per definire le autorizzazioni per l'accesso alle funzioni di consultazione in base alla tipologia di utente (Ruolo Utente).
- Deve prevedere i ruoli utente di Avvocato e CTU.
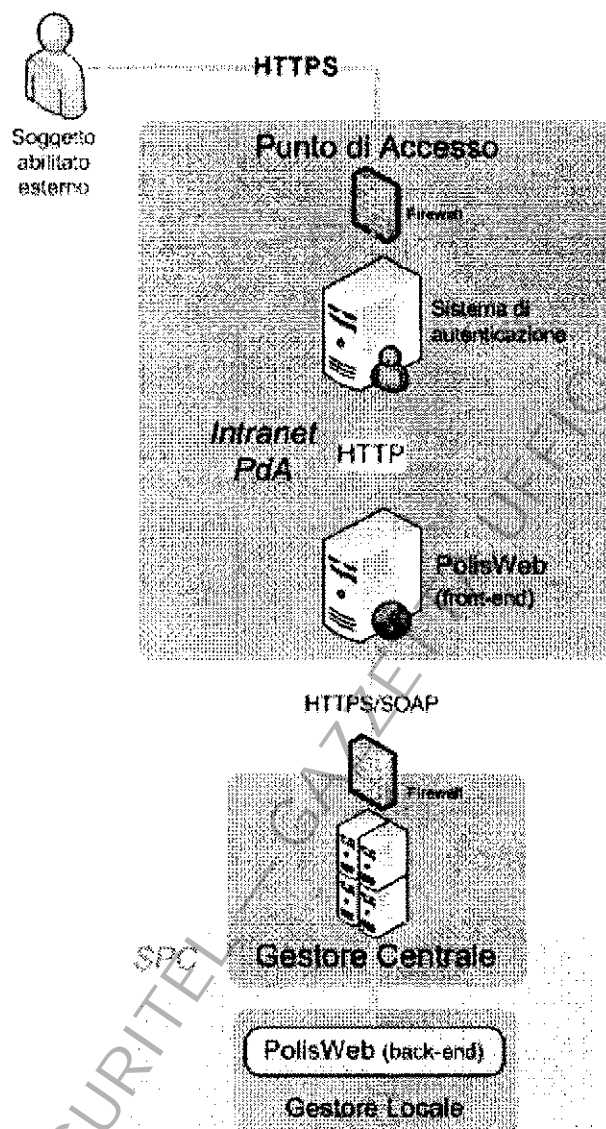
Figura 22 - Architettura di sicurezza per PolisWeb nel Punto di Accesso

- La richiesta HTTPS da PolisWeb al Gestore Centrale per l'individuazione delle informazioni di back-end presso un Ufficio Giudiziario, fornite dal Gestore Locale, va inviata all'indirizzo:

https:// NomeLogicoUfficioGiudiziario.hostgc/PathSoap

in cui:
- **NomeLogicoUfficioGiudiziario**: identificativo logico dell'Ufficio Giudiziario in base all'Ufficio indicato dall'utente nell'impostazione dei parametri di ricerca.
- **hostgc:** indirizzo telematico del Gestore Centrale (l'indirizzo del GC è gc.processotelematico.giustizia.it)
- **PathSoap:** url relativa del servizio di back-end configurato in PolisWeb e definito univocamente per l'utilizzo del Gestore Locale

Il *NomeLogicoUfficioGiudiziario*, fornito da PolisWeb al Gestore Centrale permette a quest'ultimo di individuare quale UG è interessato dalla richiesta di PolisWeb e determinare quindi l'indirizzo di rete del GL associato all'UG a cui "reindirizzare" la richiesta SOAP corrente.

2.9.2 Funzioni PolisWeb e Servizi di Back-End disponibili

Il PolisWeb deve mettere a disposizione, utilizzando i servizi di back-end di un GL presso un UG, le seguenti funzioni:

Consultazione delle informazioni gestite dai Sistemi di Gestione Registri presso l'Ufficio Giudiziario relative a:

- dati strutturati dei Fascicoli
- eventi dei Fascicoli
- scadenze dei Fascicoli
- Fascicoli Personali
- Fascicoli per l'Avvocato che deve ancora costituirsi in giudizio come difensore del convenuto.

Richiesta di informazioni su Atti dei Fascicoli:

- ricerca degli Atti, presenti nei Fascicoli, in modalità Strutturata, Testuale e Concettuale
- per ogni Atto appartenente ad un Fascicolo, deve poter essere
  - consultato il profilo dei suoi dati strutturati.
  - consultato il contenuto pdf o xml (in questo caso il contenuto viene reso visibile nel browser attraverso opportuna trasformazione in HTML)
  - effettuata la richiesta di copie cartacee o elettroniche
- le copie elettroniche degli atti richiesti sono inviate nella casella postale certificata dell'utente
- un utente deve poter consultare le richieste di copia effettuate.
- un utente deve poter indicare gli estremi di pagamento (ove previsto) relativi ad una singola Richiesta di Copia.

Richiesta di informazioni Provvedimenti nell' Archivio Giurisprudenziale:

- consultazione delle informazioni dell'Archivio Giurisprudenziale presso un Ufficio Giudiziario
- ricerca dei Provvedimenti, presenti nell'Archivio Giurisprudenziale, in modalità Strutturata, Testuale e Concettuale
- per ogni Provvedimento appartenente all'Archivio Giurisprudenziale, deve poter essere:
  - consultato il profilo dei suoi dati strutturati.
  - consultato il contenuto pdf o xml (in questo caso il contenuto viene reso visibile nel browser attraverso opportuna trasformazione in HTML)
  - effettuata la richiesta di copie cartacee o elettroniche
- le copie elettroniche dei Provvedimenti richiesti sono inviate nella casella postale certificata dell'utente.
- un utente deve poter consultare le richieste di copia effettuate.
- un utente deve poter indicare gli estremi di pagamento (ove previsto) relativi ad una singola Richiesta di Copia.

Di seguito vengono evidenziati i Servizi Soap di back-end disponibili per l'individuazione delle informazioni necessarie alle funzioni del Front-End di PolisWeb.

Si riporta per una maggiore leggibilità la descrizione degli acronimi utilizzati:

CC – Contenzioso Civile

DL – Diritto del Lavoro

AG – Archivio Giurisprudenziale

RD – Repository Documenti

RC – Richieste Copie Documenti

GL – Gestore Locale

2.10 Richieste di copie

Sul punto di accesso, tipicamente all'interno di Polis Web, dovrà essere presente un'apposita sezione per gestire le richieste di copia, nonché di accedere alla copia dei documenti rilasciati dall'Ufficio Giudiziario.

Nel flusso tra PdA e GL si distinguono due fasi:

1. esecuzione della richiesta sincrona, invocando un apposito web service esposto dal GL (WSDL pubblicato nel decreto di cui all'art. 62, comma 2);
2. invio da parte del GL del documento richiesto (o dei documenti richiesti), tramite un messaggio di posta elettronica certificata, con modalità del tutto analoghe all'invio delle comunicazioni di cancelleria (tranne il fatto che la pagina di ricezione del GC è: PTRicezioneCopie.asp).

Il contenuto del messaggio *ConsegnaCopia* è disciplinato dall'apposito XSD pubblicato nel decreto di cui all'art. 62, comma 2.

2.11 Notifiche tra difensori

2.11.1 Invio delle notifiche avvocato-avvocato

La busta predisposta dall'avvocato localmente contiene le informazioni di instradamento dell'atto (file *InfoNotifica.xml*) e l'atto informatico cifrato (file *Notifica.enc*).

Il PdA verificata la correttezza della struttura della busta caricata dall'avvocato crea un identificativo univoco (a livello PdA) dell'atto informatico da inoltrare (*IdMsgPdA*) aggiornando il file *InfoNotifica.xml*; infine crea e firma il messaggio *InoltroNotificaAvvocato* da inviare al GC.

File InfoNotifica.xml

Il file *InfoNotifica.xml* contiene le informazioni di servizio per il GC.

File Notifica.enc

Il file *Notifica.enc* è la notifica prodotta dall'Avvocato, cifrato utilizzando la chiave pubblica di cifratura dell'avvocato destinatario.

Il Punto di Accesso ed il Gestore Centrale non entrano nel merito del formato e del contenuto di questo file, che viene inviato alla CPECPT del Gestore Centrale e da questi inoltrato alla CPECPT dell'Avvocato destinatario.

2.11.2 Attestazioni temporali emesse nel flusso di invio notifiche

Il flusso di invio notifica tra difensori (nel seguito "avvocati"), disciplinato dall'art. 45 comma 8, avviene tramite posta elettronica certificata.

Esso non prevede un unico flusso dalla CPECPT mittente a CPECPT destinatario, ma risulta suddiviso in due flussi:

- Inoltro Notifica: CPECPT Mittente ↔ CPECPT GC
- Consegna Notifica: CPECPT GC ↔ CPECPT Destinatario

Questi due flussi sono collegati da un flusso di comunicazione tra server di PECPT del GC e ambiente di elaborazione del GC (in seguito indicato semplicemente con "GC").

È compito del GC individuare l'indirizzo di CPECPT del destinatario in base al codice fiscale indicato nel allegato *InfoNotifica.xml* ed inoltrare la notifica.

Di seguito si riporta il diagramma di sequenza relativo al flusso da mittente a destinatario:
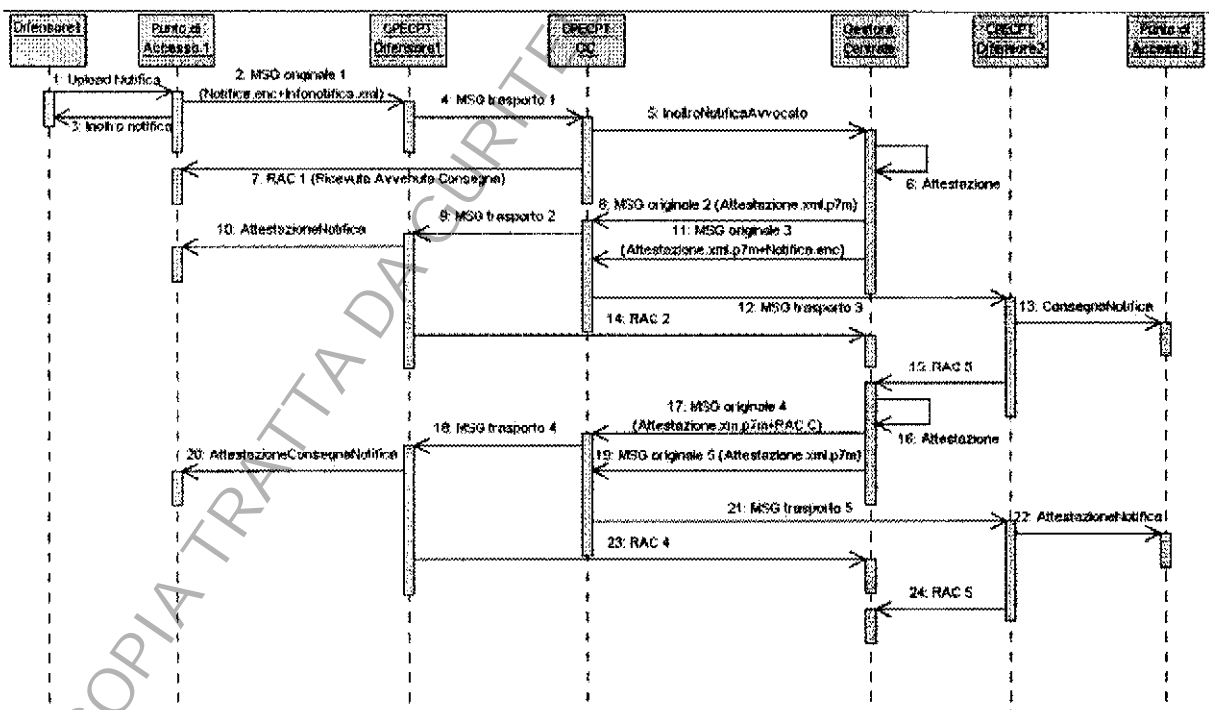
Figura 23 - diagramma di sequenza notifiche tra difensori

Di seguito si riporta l'elenco delle diverse attestazioni temporali previste dal flusso di notifica fra avvocati.

2.11.3 Attestazioni temporali ricevute a seguito dell'invio di notifiche (Avvocato mittente)

A seguito dell'invio di notifiche tra difensori, il Gestore Centrale emette delle attestazioni temporali a seguito di due eventi:

- quando riceve una notifica (formalmente corretta) da inoltrare (*AttestazioneNotifica*);
- quando riceve la ricevuta di avvenuta consegna (RAC) dal Punto di Accesso dell'avvocato destinatario. L'attestazione viene inviata all'avvocato mittente in una busta che contiene anche la Ricevuta di Avvenuta Consegna (messaggio di *AttestazioneConsegnaNotifica*).

Entrambe le attestazioni sono inviate alle caselle di posta certificata dell'avvocato mittente e del destinatario.

Nel caso della ricezione da parte dell'avvocato mittente della seconda attestazione temporale, questa è accompagnata all'interno della busta dalla Ricevuta di Avvenuta Consegna emessa dal sistema di Posta Certificata del PdA destinatario della notifica.

Nel caso di errore nel formato di uno qualsiasi dei messaggi ricevuti dal GC, viene emessa una notifica di eccezione inviata al posto del messaggio di attestazione temporale. Nel caso particolare di errore nel messaggio di notifica inviata dal mittente, il GC invia l'eccezione al mittente (messaggio di *EccezioneCertificata*) ed il flusso viene interrotto

Ricezione notifiche e relative attestazioni temporali (Avvocato destinatario)

A seguito dell'invio di notifiche tra difensori, il Gestore Centrale emette delle attestazioni temporali a seguito di due eventi:

- quando riceve una notifica (formalmente corretta) da inoltrare. L'attestazione viene inviata all'avvocato destinatario in una busta che contiene anche il messaggio di notifica stesso (messaggio di *ConsegnaNotifica*)
- quando riceve la ricevuta di avvenuta consegna (RAC) dal Punto di Accesso dell'avvocato destinatario (messaggio di *AttestazioneNotifica*).

Entrambe le attestazioni sono inviate alle caselle di posta certificata dell'avvocato mittente e del destinatario.

Controlli sui messaggi

Affinché il PdA mittente possa verificare che tutto il flusso sia avvenuto correttamente, è necessario che la RAC inviata dal punto di Accesso dell'avvocato destinatario (RAC3) sia una ricevuta completa, ovvero contenente il messaggio originale (Messaggio 3 = *Attestazione.xml.p7m* + *Notifica.enc*) e non solo l'impronta di Messaggio3 (di cui il PdA Mittente non è in possesso).

In tal modo, il PdA mittente è in grado di:

- ricavare RAC3 dal messaggio di *AttestazioneConsegnaNotifica*
- estrarre da RAC3 il file *Notifica.enc*
- verificare *Notifica.enc* così ricavato con quello originario spedito.

Per attestare il corretto scambio di messaggi tra CPECPT del GC e ambiente di elaborazione del GC, è necessario che entrambi i PdA (mittente e destinatario) effettuino i controlli di corrispondenza delle impronte contenute nelle attestazioni temporali ricevute (elencate sopra) rispetto ai relativi messaggi originali.

2.12 Funzionalità di accesso ai registri degli indirizzi elettronici

Il Gestore Centrale mantiene aggiornato il Registro Generale degli Indirizzi Elettronici (ReGIndE), dove è registrato l'elenco di tutti gli indirizzi elettronici attivati dai Punti di Accesso. Sul Gestore Centrale viene inoltre mantenuto un registro degli Uffici Giudiziari, in cui sono registrati i dati di tutti i Tribunali che partecipano al Processo Telematico.

Il Gestore Centrale mette a disposizione un servizio che consente di interrogare i registri accedendo in modalità LDAP.

2.12.1 Accesso al REGIndE per il reperimento di indirizzi e certificati degli avvocati

Il registro generale degli indirizzi elettronici sul Gestore Centrale contiene gli indirizzi e i dati di tutti gli avvocati e dei CTU; la struttura LDAP di accesso al REGIndE è riportata nel decreto di cui all'art. 62, comma 2.

Ad ogni indirizzo elettronico di persona fisica sono associate le informazioni indicate in art. 13, comma 3, 4.

Per inviare comunicazioni e notifiche ad altri avvocati, ciascun avvocato deve conoscerne il codice fiscale ed eventualmente la chiave pubblica di cifratura del destinatario.

Ogni Punto di Accesso deve mettere a disposizione una funzione di consultazione del ReGIndE per il reperimento di chiavi pubbliche dei certificati di cifratura, utili per inviare comunicazioni e notifiche ad altri avvocati.

2.12.2 Accesso al Registro degli Uffici Giudiziari

In fase di redazione e preparazione degli atti o dei documenti da inviare verso un Ufficio Giudiziario, gli avvocati devono avere a propria disposizione sul posto di lavoro il codice identificativo dell'Ufficio destinatario e, per inviare un atto cifrato, anche la chiave pubblica di cifratura.

Il Gestore Centrale mantiene un registro degli Uffici Giudiziari, in cui sono registrati i dati di tutti i Tribunali che partecipano al Processo Telematico e mette a disposizione un servizio di interrogazione del registro, in modalità LDAP, la cui struttura è riportata nel decreto di cui all'art. 62, comma 2.

3 REQUISITI TECNICI SPECIFICI DEL PUNTO DI ACCESSO

3.1 COLLEGAMENTO CON IL GESTORE CENTRALE

I punti di accesso sono attestati su una rete privata virtuale dedicata al processo civile telematico, di cui fa parte il Gestore Centrale, realizzata anche nell'ambito di contratti per la fornitura di servizi di connettività previsti per le pubbliche amministrazioni.

3.2 CONTROLLI SUI MESSAGGI

Il PdA è tenuto ad effettuare controlli formali su tutti i messaggi in ingresso (sia da parte del GC che degli utenti esterni), ed in particolare:

1. effettuare controlli antivirus;
2. ove prevista, verificare la validità del certificato di firma del GC e che i messaggi non siano stati modificati (tramite controllo dell'Hash);
3. controllare che gli eventi temporali, ove previsti, siano ragionevolmente corretti: è in particolare richiesto l'allineamento del proprio orologio di sistema rispetto all'orologio del GC; in particolare è tenuto a controllare la validità della data di attestazione temporale (compresa tra la data di deposito e la data di ricezione dell'attestazione temporale stessa da parte del PdA) con tolleranza di disallineamento di 1 minuto;
4. nel caso di messaggi relativi al flusso di deposito verificare la correttezza di tutti gli identificatori di messaggio, utente, PdA, ecc...;
5. alla ricezione di attestazione temporale ed esito atto, verificare la corrispondenza dei valori dell'impronta rispetto al deposito effettuato.

Ciascun PdA può definire autonomamente le procedure di caricamento degli atti a partire dalla postazione dell'utente esterno, automatizzando o meno la compilazione delle informazioni di spedizione.

Nel caso in cui vengano estrapolate dalla busta caricata deve essere verificato che la busta sia destinata ad un UG conosciuto.

3.3 TRACCIABILITÀ

Il PdA deve consentire la tracciabilità dello stato dei pacchetti inviati al GC, evidenziando in particolare:

- la ricezione di attestazione temporale: essendo una ricevuta "a valore legale", il PdA informa l'utente della ricezione anche in caso di non conformità dei dati (ad esempio validità temporale, valore del campo impronta...) fornendo informazioni relative ad anomalie riscontrate.
- La ricezione di una notifica di eccezione

In caso l'attestazione presenti qualche anomalia (ad esempio qualche campo non corretto) l'Amministratore del PdA è tenuto a segnalare opportunamente l'anomalia ed in individuarne la causa.

3.4 *Comportamento in caso di mancanza di risposta dal GC*

In caso di mancata risposta da parte del GC, al fine di evitare rischi di duplicazione di pacchetti inviati, il PdA non deve procedere al reinvio automatico.

In tale caso, pertanto, il referente del Punto di Accesso è tenuto a segnalare prontamente la problematica al servizio di monitoraggio del Gestore Centrale, utilizzando le modalità definite dalla DGSIA.

3.5 *Statistiche di Utilizzo dei Servizi*

A norma dell'art. 29, I PdA dovranno essere in grado di inviare, su richiesta del Ministero della Giustizia, le statistiche di utilizzo relativamente ai servizi messi a disposizione degli utenti abilitati esterni,

I formati dei log richiesti verranno stabiliti dalla DGSIA in accordo diretto con i PdA.

3.6 *Codifica degli errori riportati dal Gestore Centrale*

La seguente tabella riporta l'anagrafica degli errori che possono essere inseriti dal Gestore Centrale nei messaggi di notifica eccezione.

Codice	*Descrizione*
E0101	L'element ?? non e' valorizzato
E0102	L'element ?? non ha un formato valido.
E0103	L'element ?? non ha un valore ammesso.
E0104	L'attributo ?? non ha un valore ammesso.
E0200	Il certificato ?? non e' valido o e' scaduto.
E0201	Il Punto di Accesso presente in InfoInoltro non corrisponde con il titolare del Certificato di firma.
E0202	L'element ?? non e' integro.
E0203	Il file ?? non dovrebbe essere presente.
E0204	L'Utente risulta abilitato su altro PDA.
E0205	Il Punto di Accesso (??) presente in InfoInoltro non corrisponde a quello del Mittente.
E0300	Il messaggio primario ricevuto non e' integro.
E0301	La struttura di ?? non e' valida.
E0303	Il messaggio primario ricevuto non e' integro. La parte ?? e' mancante.
E0304	Il content-type del messaggio non e' riconosciuto.
E0400	L'identificativo del messaggio ricevuto non e' univoco (IdMsgPdA).
E0401	Il Mittente del messaggio (CF = ??) non e' autorizzato al Processo Telematico.
E0402	Il destinatario del messaggio (InoltroAtto/Destinatario = ??) e' sconosciuto o non e' consentito.
E0403	L'Avvocato certificato (CF = ??) non e' il Mittente del messaggio (InoltroAtto/Mittente).
E0405	Il ?? e' sconosciuto.
E0406	Il Destinatario del messaggio (CF = ??) non e' autorizzato al Processo Telematico.
E0500	La certificazione allegata non contiene la firma.
E0501	La certificazione allegata non corrisponde al relativo DTD.

E0502	Il codice fiscale contenuto nella Certificazione non corrisponde con il codice fiscale di InfoInoltro.
E0503	La data riportata dalla certificazione non corrisponde con la data odierna.
E0504	Il PdA riportato nella certificazione non coincide con quello che ha inviato il messaggio.
E0505	L'ordine riportato nella certificazione non esiste.
E0506	Lo status dell'Avvocato riportato nella certificazione non e' corretto.
E0600	Informazioni mancanti nella ComunicazioneUG.
E0601	Codice del Gestore Locale sconosciuto.
E0602	Codice Fiscale del destinatario sconosciuto.
E0603	Impossibile recuperare la ComunicazioneUG.
E0604	Identificativo duplicato.
E0605	Struttura ComunicazioneUG errata.
E0606	Messaggio non riconosciuto.
E0607	Il nodo 'esitoAtto' non punta ad alcun allegato.
E0608	Status Difensore non presente.
E0609	Formato Codice Fiscale non valido.
E0700	Errore nella verifica della firma della ComunicazioneIndirizzi.xml.p7m.
E0701	Firmatario della ComunicazioneIndirizzi.xml.p7m non identificato.
E0702	Rilevati errori nella validazione dei dati del Soggetto Esterno.
E0703	La ComunicazioneIndirizzi allegata non corrisponde al relativo DTD.

Il codice "??" è, di volta in volta, sostituito dal valore specifico.

08A05320

ITALO ORMANNI, *direttore*

ALFONSO ANDRIANI, *redattore*
DELIA CHIARA, *vice redattore*

(G803164/1) Roma, 2008 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

CANONI DI ABBONAMENTO ANNO 2008 (salvo conguaglio) (*)

GAZZETTA UFFICIALE - PARTE I (legislativa)

		CANONE DI ABBONAMENTO	
Tipo A	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:		
	(di cui spese di spedizione € 257,04)	- annuale	€ **438,00**
	(di cui spese di spedizione € 128,52)	- semestrale	€ **239,00**
Tipo A1	Abbonamento ai fascicoli della serie generale, inclusi i soli supplementi ordinari contenenti i provvedimenti legislativi:		
	(di cui spese di spedizione € 132,57)	- annuale	€ **309,00**
	(di cui spese di spedizione € 66,28)	- semestrale	€ **167,00**
Tipo B	Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale:		
	(di cui spese di spedizione € 19,29)	- annuale	€ **68,00**
	(di cui spese di spedizione € 9,64)	- semestrale	€ **43,00**
Tipo C	Abbonamento ai fascicoli della serie speciale destinata agli atti della CE:		
	(di cui spese di spedizione € 41,27)	- annuale	€ **168,00**
	(di cui spese di spedizione € 20,63)	- semestrale	€ **91,00**
Tipo D	Abbonamento ai fascicoli della serie destinata alle leggi e regolamenti regionali:		
	(di cui spese di spedizione € 15,31)	- annuale	€ **65,00**
	(di cui spese di spedizione € 7,65)	- semestrale	€ **40,00**
Tipo E	Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:		
	(di cui spese di spedizione € 50,02)	- annuale	€ **167,00**
	(di cui spese di spedizione € 25,01)	- semestrale	€ **90,00**
Tipo F	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari, ed ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 383,93)	- annuale	€ **819,00**
	(di cui spese di spedizione € 191,46)	- semestrale	€ **431,00**
Tipo F1	Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari con i provvedimenti legislativi e ai fascicoli delle quattro serie speciali:		
	(di cui spese di spedizione € 264,45)	- annuale	€ **682,00**
	(di cui spese di spedizione € 132,22)	- semestrale	€ **357,00**

N.B.: L'abbonamento alla GURI tipo A, A1, F, F1 comprende gli indici mensili
Integrando con la somma di € 80,00 il versamento relativo al tipo di abbonamento alla *Gazzetta Ufficiale* - parte prima - prescelto, si riceverà anche l'**Indice Repertorio Annuale Cronologico per materie anno 2008.**

CONTO RIASSUNTIVO DEL TESORO

Abbonamento annuo (incluse spese di spedizione) € **56,00**

PREZZI DI VENDITA A FASCICOLI
(Oltre le spese di spedizione)

Prezzi di vendita:		
	serie generale	€ 1,00
	serie speciali (escluso concorsi), ogni 16 pagine o frazione	€ 1,00
	fascicolo serie speciale, *concorsi*, prezzo unico	€ 1,50
	supplementi (ordinari e straordinari), ogni 16 pagine o frazione	€ 1,00
	fascicolo Bollettino Estrazioni, ogni 16 pagine o frazione	€ 1,00
	fascicolo Conto Riassuntivo del Tesoro, prezzo unico	€ 6,00

I.V.A. 4% a carico dell'Editore

5ª SERIE SPECIALE - CONTRATTI ED APPALTI

(di cui spese di spedizione € 127,00)	- annuale	€ **295,00**
(di cui spese di spedizione € 73,00)	- semestrale	€ **162,00**

GAZZETTA UFFICIALE - PARTE II

(di cui spese di spedizione € 39,40)	- annuale	€ **85,00**
(di cui spese di spedizione € 20,60)	- semestrale	€ **53,00**

Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione) € 1,00
I.V.A. 20% inclusa

RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI

Abbonamento annuo		€ **190,00**
Abbonamento annuo per regioni, province e comuni - SCONTO 5%		€ **180,50**
Volume separato (oltre le spese di spedizione)	€ 18,00	

I.V.A. 4% a carico dell'Editore

Per l'estero i prezzi di vendita, in abbonamento ed a fascicoli separati, anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso. Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli, vengono stabilite, di volta in volta, in base alle copie richieste.

N.B. - Gli abbonamenti annui decorrono dal 1° gennaio al 31 dicembre, i semestrali dal 1° gennaio al 30 giugno e dal 1° luglio al 31 dicembre.

RESTANO CONFERMATI GLI SCONTI IN USO APPLICATI AI SOLI COSTI DI ABBONAMENTO

ABBONAMENTI UFFICI STATALI
Resta confermata la riduzione del 52% applicata sul solo costo di abbonamento

* tariffe postali di cui al Decreto 13 novembre 2002 (G.U. n. 289/2002) e D.P.C.M. 27 novembre 2002 n. 294 (G.U. 1/2003) per soggetti iscritti al R.O.C.

€ 5,00